

10/502048

P25670.P03

DT04 Rec'd PCT/PTO 30 JUL 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Masayuki ORIHASHI et al.
Appl. No: : Not Yet Assigned (National Phase of PCT/JP03/02174) PCT Branch
Filed : Concurrently Herewith (I.A. Filed February 28, 2002)
For : COMMUNICATION APPARATUS AND COMMUNICATION SYSTEM

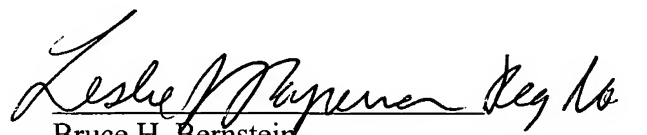
CLAIM OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Japanese Application Nos. 2002-54064, filed February 28, 2002; 2002-132068, filed May 7, 20002; and 2003-48364, filed February 25, 2003. The International Bureau already should have sent certified copies of the Japanese applications to the United States designated office. If the certified copies have not arrived, please contact the undersigned.

Respectfully submitted,
Masayuki ORIHASHI et al.


Bruce H. Bernstein
Reg. No. 29,027
33,329

July 21, 2004
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

日本国特許庁
JAPAN PATENT OFFICE

PCT/JP03/02174
27.02.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

RECEIVED	
21 MAR 2003	
WIPO	PCT

出願年月日
Date of Application:

2002年 2月28日

出願番号
Application Number:

特願2002-054064

[ST.10/C]:

[JP2002-054064]

出願人
Applicant(s):

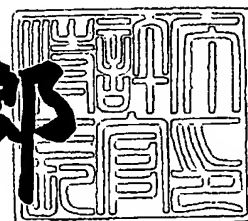
松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2002年12月17日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2002-3099902

【書類名】 特許願

【整理番号】 2931030102

【提出日】 平成14年 2月28日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 7/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 折橋 雅之

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 村上 豊

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 安倍 克明

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 松岡 昭彦

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 通信装置

【特許請求の範囲】

【請求項 1】 通信に用いられ、信号を受信し受信信号を出力する受信部と、前記受信信号を復調し受信情報を出力する復調部と、前記受信信号から伝搬特性を推定し伝搬情報を出力する伝搬推定部と、前記伝搬情報を暗号鍵に符号化する符号部と、符号化された前記暗号鍵を用いて前記受信情報の暗号を復号し復号情報を出力する復号部とを有する通信装置。

【請求項 2】 通信に用いられ、信号を受信し受信信号を出力する受信部と、前記受信信号を復調し受信情報を出力する復調部と、前記受信信号から伝搬特性を推定し伝搬情報を出力する伝搬推定部と、前記伝搬情報を暗号鍵に符号化する符号部と、符号化された前記暗号鍵を用いて前記受信情報の暗号を復号し復号情報を出力する復号部と、前記暗号鍵を用いて送信情報の暗号化を行い暗号情報を出力する暗号化部と、前記暗号情報を変調した変調信号を出力する変調部と、変調信号を出力する送信部とを有する通信装置。

【請求項 3】 通信に用いられ、信号を受信し受信信号を出力する受信部と、前記受信信号を復調し受信情報を出力する復調部と、前記受信信号から伝搬特性を推定し伝搬情報を出力する伝搬推定部と、前記伝搬情報を暗号鍵に符号化する符号部と、符号化された前記暗号鍵を用いて前記受信情報の暗号を復号し復号情報を出力する復号部と、前記暗号鍵を用いて送信情報の暗号化を行い暗号情報を出力する暗号化部と、前記暗号鍵と前記伝搬情報から出力伝搬制御信号を出力する伝搬制御部と、前記暗号情報を前記出力伝搬制御信号に基づき変調し、送信する送信・変調部とを有する通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はデジタル通信に用いられる技術であって、特にセキュリティに関する技術である。

【0002】

【従来の技術】

デジタル無線通信は、その技術の発展により通信分野の重要な位置を占めるようになってきている。しかしながら、無線通信が公共財である電波空間を利用したものであるため、第3者による受信が可能であるといった根本的な課題を内包している。このため、常に通信内容が第3者により傍受され、情報が漏洩する危険性をはらんでいた。

【0003】

このような問題を解決するために、通信情報を暗号化するなどして傍受されても情報が漏洩しないような処理を行っているのが現状である。

【0004】

【本発明が解決しようとする課題】

情報の暗号化は、様々な分野で研究され、また様々な分野で応用されている。これは、通信システムを変更しなくても一定のセキュリティが確保できるといった大きな特長によるところが大きい。

【0005】

しかしながら、この方法では第3者による傍受を防ぐことはできないため、時間をかけることによって、傍受した受信情報から解読されてしまうと言った課題がある。

【0006】

【課題を解決するための手段】

これらの問題を解決するため、伝搬路遅延などの伝搬路環境を用いた通信方式を提案する。伝搬路環境は通信間の絶対的、あるいは相対的な状況により変動するため、送信局からみると受信局を特定する1つのパラメータとなる。例えば、送信局が伝搬路遅延までを含めて、受信局に対して同期した通信信号を送信する場合を考える。受信局では、同期した信号が受信されるため、同期の必要はなくそのまま受信信号を復調すればよい。一方、第3者が受信した受信信号では、どの時刻を基準に復調をすればよいのか知ることができないため、受信はできても復調はできないことになる。

【0007】

この様に、本発明を用いることで大きな通信システムの変更をすることなしに、高いセキュリティを提供する事が可能になる。

【 0 0 0 8 】

【発明の実施の形態】

本発明の請求項 1 に記載の発明は、通信に用いられ、信号を受信し受信信号を出力する受信部と、前記受信信号を復調し受信情報を出力する復調部と、前記受信信号から伝搬特性を推定し伝搬情報を出力する伝搬推定部と、前記伝搬情報を暗号鍵に符号化する符号部と、符号化された前記暗号鍵を用いて前記受信情報の暗号を復号し復号情報を出力する復号部とを有する通信装置であり、伝搬特性を暗号鍵とすることで第 3 者への情報漏洩を抑える通信を可能にするといった作用を有する。

【 0 0 0 9 】

本発明の請求項 2 に記載の発明は、通信に用いられ、信号を受信し受信信号を出力する受信部と、前記受信信号を復調し受信情報を出力する復調部と、前記受信信号から伝搬特性を推定し伝搬情報を出力する伝搬推定部と、前記伝搬情報を暗号鍵に符号化する符号部と、符号化された前記暗号鍵を用いて前記受信情報の暗号を復号し復号情報を出力する復号部と、前記暗号鍵を用いて送信情報の暗号化を行い暗号情報を出力する暗号化部と、前記暗号情報を変調した変調信号を出力する変調部と、変調信号を出力する送信部とを有する通信装置であり、伝搬特性を送受信時の暗号鍵とすることで第 3 者への情報漏洩を抑える送受信通信を可能にするといった作用を有する。

【 0 0 1 0 】

本発明の請求項 3 に記載の発明は、通信に用いられ、信号を受信し受信信号を出力する受信部と、前記受信信号を復調し受信情報を出力する復調部と、前記受信信号から伝搬特性を推定し伝搬情報を出力する伝搬推定部と、前記伝搬情報を暗号鍵に符号化する符号部と、符号化された前記暗号鍵を用いて前記受信情報の暗号を復号し復号情報を出力する復号部と、前記暗号鍵を用いて送信情報の暗号化を行い暗号情報を出力する暗号化部と、前記暗号鍵と前記伝搬情報から出力伝搬制御信号を出力する伝搬制御部と、前記暗号情報を前記出力伝搬制御信号に基

づき変調し、送信する送信・変調部とを有する通信装置であり、伝搬特性を送受信時の暗号鍵とすると共に、送信信号を暗号鍵に基づき伝搬制御を行うことで安定した通信の提供を可能にするといった作用を有する。

【 0 0 1 1 】

以下、本発明の実施の形態について図面を用いて説明する。

【 0 0 1 2 】

(実施の形態 1)

伝搬情報をセキュリティの暗号鍵情報として利用する発明について図 1、図 2 および図 3 を用いて説明する。図 1 は暗号受信装置の具体的構成を示し、図 2 は暗号送受信装置の具体的構成を示したものである。図 3 は端末間の通信手続きを記述したものである。ここでは便宜上、図 3 中の基地局を図 2 に示した暗号送受信装置、端末を図 1 で示した暗号受信装置であるものとして説明を行うが、その組合せを制限するものではなく、両者が図 2 で示す暗号送受信装置であっても構わない。

【 0 0 1 3 】

図 1 はアンテナ 1 0 1 と、暗号受信部 1 5 3 と、送信部 1 5 1 とで構成されている。1 5 3 は受信した R F 信号から伝搬状態を推定し、これを暗号鍵として暗号の復号を行いセキュリティデータを出力する暗号受信部であり、受信復調部 1 5 0 と、暗号鍵生成部 1 5 1 と、復号化部 1 0 7 とで構成されている。1 5 2 は基準 R F 信号を出力する送信変調部であり、基準信号生成部 1 0 8、送信部 1 0 9 とからなる。1 0 1 は電波を受信・送信し R F 信号を入出力するアンテナ、1 5 0 は R F 信号を入力し、伝搬情報と復調情報とを出力する受信復調部であり、受信部 1 0 2、伝搬推定部 1 0 3、復調部 1 0 4 とからなる。

【 0 0 1 4 】

1 0 2 は R F 信号と伝搬情報を入力し、R F 信号を適切な受信状態に制御し、受信信号を出力する受信部であり、1 0 3 は受信信号から伝搬特性を推定し伝搬情報出力する伝搬推定部であり、1 0 4 は受信信号と伝搬情報とから適切な復調を行い復調情報出力する復調部である。1 5 1 は伝搬情報を入力し暗号鍵情報出力する暗号鍵生成部であり、符号化部 1 0 5 とバッファ部 1 0 6 とで構成

されている。

【0015】

105は伝搬情報から特徴を抽出し暗号鍵を生成・出力する符号化部であり、106は符号化された暗号鍵を記憶し、記憶した暗号鍵情報を出力するバッファ部である。107は暗号鍵情報と復調情報とを入力し、暗号鍵情報から復調情報の暗号を復号化しセキュリティデータを出力する復号化部である。108は予め定められた基準信号を生成し出力する基準信号生成部であり、109は基準信号を入力しRF信号に変調・出力する送信部である。

【0016】

図2はアンテナ201と、暗号受信部253と、暗号送信部254とで構成されている。アンテナ201および暗号受信部253は、図1中での対応する部位と同等の機能を有している。254はセキュリティデータと暗号鍵情報とを入力し、伝搬推定用の基準信号と、暗号鍵情報とセキュリティデータとから予め定められた方法により暗号化される暗号化情報と、を切り換えて変調・出力する暗号送信部であり、送信変調部251と、基準信号生成部208と、暗号化部209と、切換部210とで構成される。

【0017】

252は選択された通信情報を変調しRF信号を出力する変調送信部であり、変調部211と送信部212とから構成されている。208は予め定められた基準信号を生成し出力する基準信号生成部であり、209は暗号鍵情報とセキュリティデータとを入力し、暗号鍵情報からセキュリティデータを暗号化し、暗号情報を生成・出力する暗号化部である。210は基準信号と暗号情報とを入力し、両者のうち1つを選択、通信情報を出力する選択部であり、211は選択された通信情報を変調し変調信号を出力する変調部であり、212は変調信号を送信するRF信号に変換・出力する送信部である。

【0018】

以上のように構成された基地局（図2に示される暗号送受信装置）と端末（図1に示される暗号受信装置）とは、図3のような手順で通信を行っている。

【0019】

以下、図1に示された装置の動作を説明する。アンテナ101は、電波を受信しRF信号を出力する。受信されたRF信号は、受信復調部150に入力され伝搬情報と復調情報とが出力される。まず、受信部102はRF信号と伝搬情報を入力し、伝搬情報に従い、ゲインを一定に保ったり、周波数・時間ずれを修正したりすることで受信状態を最適に保つように制御しながら受信信号を出力する。伝搬推定部103は受信信号を入力し、受信時刻、伝搬時間、周波数状態、偏波状態、受信電力、マルチパス状態、位相状態、伝搬歪などを検出する。

【0020】

それぞれの状態は、受信復調パラメータ用に伝搬情報として受信部102、復調部104へと送出されると同時に、暗号鍵生成部151へも送出される。復調部104は、受信信号と伝搬情報とを入力し、伝搬情報に従って受信信号からマルチパス成分を除去、或いは位相の調整などを行いながら復調し、復調情報104を出力する。暗号鍵生成部151は受信復調部150から出力された伝搬情報から伝搬状態の特徴を抽出し、暗号鍵を生成・記憶し、暗号鍵情報を出力する。

【0021】

符号化部105は伝搬推定部103から出力された伝搬情報を入力し、その中から受信信号の伝搬状態の特徴を抽出する。例えば、マルチパス状態を例に挙げると、複数の伝搬路により形成されるマルチパス伝搬において、そのマルチパス特性は相関関数などを用いて検出することが可能である。

【0022】

このようにして求められたマルチパスの電界情報のうち、最大のパワーを検出したパス成分の遅延時間とパワーとから予め定められた方法に従って符号化を行い、暗号化に用いる暗号鍵を生成・出力する。生成された暗号鍵は、バッファ部106で入力され記憶されて、暗号鍵情報が出力される。復号化部107は、復調情報と暗号鍵情報を入力し予め定められた方法に従って復調情報を復号し、セキュリティデータを出力する。送信部152は基準信号を生成した後、変調しRF信号を出力する。基準信号生成部108は、通信対象の相手端末に対して伝搬状態を推定するための基準信号を生成し、これを出力する。送信変調部109は基準信号を入力し、変調・周波数変換などによりRF信号を出力する。出力され

たRF信号は、アンテナ101から放射される。

【0023】

図2に示された装置の動作を説明する。ここでは、図1に示した装置からの相違点のみを示す。

【0024】

アンテナ201から入力されたRF信号が、復号化207を通じて復号されセキュリティデータが出力されるまでの暗号受信部253は、図1の対応する部位と同一の構成である。暗号送信部254は、暗号鍵情報とセキュリティデータを入力し、送信するRF信号を出力する。基準信号生成部208は、通信対象の相手端末に対して伝搬状態を推定するための基準信号を生成し、出力する。暗号化部209は、暗号鍵情報とセキュリティデータとを入力し、予め定められた方法に従って暗号化した暗号化情報を出力する。

【0025】

切換部210は、基準信号生成部208から入力される基準信号と、暗号化部209から入力される暗号化情報の一方を選択し選択された通信情報を出力する。選択された通信情報は、送信変調部252により変調され送信信号に変換されてRF信号を出力する。まず、通信情報は変調部211に入力され所定の変調が施された変調信号が出力される。次に、変調信号は送信部212へ入力され、RF信号に変換されて出力される。このRF信号はアンテナ201を介して放射される。

【0026】

以上の動作を、通信手順の観点から図3を用いて説明する。

【0027】

(0) 基地局、端末：初期化

基地局、端末共に、電源が投入された直後、或いは特定の信号を受けて初期状態にセットされる。同時に、周波数や時間同期などの状態は事前に定められた手順に従ってセットされる。

【0028】

以上のこれらの初期動作が終了した一定時間後、基地局は一定時間毎に制御情

報を制御信号に載せて送信する。

【0029】

一方、端末は初期動作が終了した後、制御信号のサーチを始める。端末が基地局から送信した制御信号を受信すると、その時刻、周波数などを検出してシステムが保有する時刻・周波数に同期する（システム同期）。システム同期が正常に終了した後、端末はその存在を基地局に通知するために登録要求信号を送信する。基地局は、端末からの登録要求に対して、登録許可信号を送信することで端末の登録許可を行う。

【0030】

(1) 基地局：第1基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第1基準信号として出力する。具体的には、切換部210は基準信号生成部208で生成される基準信号を選択し、送信変調部252へ出力する。送信変調部252は選択された通信情報をRF信号としてアンテナ201から放射する。

【0031】

端末では、基地局からの信号を待っており、伝搬推定部103は受信した受信信号から第1基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。符号化部105は、伝搬推定部103からの伝搬情報を入力し、伝搬状態の特徴抽出をおこなう。次に抽出した特徴情報を用いて暗号鍵への変換を行う。この部分の動作は別途詳細に説明する。この符号化部105が抽出する特徴や、それを暗号鍵へ変換する方法については基地局と端末の間で予め共有しておくものとする。変換された暗号鍵はバッファ部106に保持され暗号鍵情報が出力される。この暗号鍵を第1鍵として基地局は以降の通信の暗号鍵とする。

【0032】

(2) 端末：第2基準信号送信

端末は、(1)と同様に基地局で行う伝搬推定用の基準信号を第2基準信号として出力する。

【0033】

基地局では、端末からの信号を受信すると第2基準信号を検出し、伝搬推定部

203は受信信号と既知信号である基準信号とから伝搬推定を行う。(1)と同様、伝搬推定部203が出力する伝搬情報は、符号化部205によって暗号鍵へと変換され、バッファ部206で暗号鍵情報が保持、出力される。この暗号鍵を第2鍵として端末は以降の通信の暗号鍵とする。

【0034】

(3) 基地局：暗号送信

基地局は、切換部210の状態を、暗号化部209から出力される暗号化情報を選択するように切り換える。暗号化部209は(2)で得られた第2鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化情報を出力する。暗号化情報は切換部210で選択され、通信情報が送信変調部252へと出力される。送信変調部252は通信情報を変調し、RF信号としてアンテナ201から暗号化信号を放射する。

【0035】

端末は、暗号化信号を受信すると受信復調部150が受信信号を復調情報へと復調する。復号化部107は復調情報と(1)で求めた第1鍵を用い、予め定められた方法によって暗号の復号化を行いセキュリティデータを出力する。以下、(3)の暗号通信や通常の通信を繰り返す。

【0036】

さて、通信端末間で形成される伝搬路はその相対的な位置や空間形状、反射物などにより一意に決まり、それは基地局から端末に対して形成される伝搬状態と、端末から基地局に対して形成される伝搬状態は光伝搬の相反性により同一であることが知られている。このことは、(1)で求められる伝搬状態と(2)で求められる伝搬状態(例えば、遅延プロファイルなど)は同一の結果が求まることとなることがわかる。また、基地局と端末の間では、予め伝搬情報から暗号鍵へと変換する手順を共有してある。則ち、(1)で得られる暗号鍵(第1鍵)と(2)で得られた暗号鍵(第2鍵)は同一となり、通信端末間においては共有鍵として用いることが可能な状態となっている。この結果、(3)の通信手順においては共有鍵で暗号化・復号化を行うこととなり、基地局で暗号化された情報は端末で正常に復号化されることになる。

【 0 0 3 7 】

さて、この状況で全通信を第3者が第3の端末を用いて傍受した場合を考える。先に説明したとおり、伝搬路は基地局と端末との間で形成される伝搬空間で求まるものである。このため、基地局や端末から物理的に異なった位置で(1)から(3)までの通信を観察している場合、第3の端末と基地局或いは端末間で形成される伝搬特性は、(1)や(2)で求められるそれとは異なってくる。その上、基地局と端末間では暗号化の為の鍵の授受を行っているわけではないため、第3の端末がこれを知ることは出来ない。

【 0 0 3 8 】

このことから、通信の物理層において高いセキュリティを確保できることが分かる。また、これらの処理は基本的に従来の算術的な手法を用いた暗号化、復号化とは独立して行うことが可能であるため、従来技術に加えて本発明を実施することでより高いセキュリティが期待できるといった有利な特長を有する。

【 0 0 3 9 】

この説明において、初期化作業である(0)について説明を行ったが、これは一般的な運用を想定したものであり、本発明に必要な手続きではない。また、(1)や(2)で基準信号を送信することで、互いの伝搬状態を推定するとしたが、これは一般に既知信号としての基準信号を用いた方が精度を高く推定できるためであって、伝搬推定では特に基準信号を用いなくても可能なことはいうまでもない。換言すれば、例えば(0)で行っている制御信号、登録要求信号や登録許可信号などを利用して伝搬推定を行うことも可能である。

【 0 0 4 0 】

以上の発明は、伝搬状態を暗号鍵として利用することを特徴としているため、基地局や端末の移動が発生すると、問題が生ずる虞がある。この場合、図3に示した(1')、(2')、(3')のように繰り返し基準信号の送受信を行うことで、この問題を回避することも可能である。

【 0 0 4 1 】

ここでは、伝搬状態を示すパラメータとして遅延プロファイルを用いたが、偏波面や旋回方向などの偏波状態を用いたり、位相情報を用いたり、伝搬遅延時間

を用いたり、到来方向推定情報を用いたり、受信電力情報を用いたり、或いは、様々なパラメータの組み合わせを用いたりすることも考えられる。こうすることで、第3の端末の観測がより複雑化するため高度なセキュリティを確保できる。特に、偏波や位相を用いることで、それらが伝搬環境に大きく左右されることから、他の端末からの推定を一層困難にするといった特徴を有する。

【0042】

さらに、複数のアンテナ201に複数のアンテナエレメントで構成するアレイアンテナ構造を適用することで、伝搬推定のパラメータとして到来方向の要素を付加することができる。こうすることでより柔軟なシステムを構成が可能となる。

以上の説明においては、変調方式、多重化方式について説明していないが、本方式は原理的にどの変調方式にも適用できることは明白であり、現在行われているPSK変調、QAM変調、スターQAM変調、或いはTDMA、FDMA、SS(FHやCDMA)、OFDMなどあらゆるものに適用可能である。

【0043】

通信手順で、基準信号を送信する際、第1基準信号の送信と第2基準信号の送信を行っているが、両者はどちらが先に実施されても本方式に影響を与えるものではないことは明白である。また、通信手順の中で基準信号を別途通信しているが、これは、図9のフレーム構成(b)、(c)のように、データストリームの中に基準信号を挿入することで、(1)と(3)の手順を同時に実施することができるといった有利な特長を有することが出来る。

【0044】

(実施の形態2)

伝搬推定と暗号鍵への変換方法について、図1および図6を用いて説明する。

【0045】

ここでは伝搬状態を示すパラメータとして代表的な遅延プロファイルを扱うものとして説明する。この遅延プロファイルは、各パス成分の遅延時間と、パワー、位相などが含まれている。ここでは、パス成分の遅延時間とパワーとを扱った例を示す。

【0046】

図1中の伝搬推定部103は基準信号が含まれる受信信号を取り出し、伝搬状態の推定を行う。伝搬状態として遅延プロファイルを求める場合、遅延プロファイルは基となる信号と受信した信号との相関で求められることが知られている。この場合、伝搬推定部103は既知信号である基準信号を用いて、その信号系列と受信信号系列の相関値を算出することで遅延プロファイルが得られる。

【0047】

このようにして得られた伝搬情報は符号化部105によってその特徴が抽出される。特徴抽出の例としてベクトル量子化手法を用いるものが考えられる。これは、代表的な遅延プロファイルのテンプレートを量子化ベクトルとして参照テーブル上に幾つか用意しておき、更に各量子化ベクトルに対応させた暗号鍵を参照テーブル上に格納しておく。符号化部105は、このように用意しておいた参照テーブルから伝搬推定部103が推定した結果と照合し、最も類似性の高い遅延プロファイルのテンプレートに対応する暗号鍵を選択・出力する。

【0048】

以上、伝搬状態を推定し、暗号鍵へと符号化する方法について説明したが、図6を用いてさらに詳細に説明する。

【0049】

図6中の650は伝搬推定部、651は符号化部を示している。これらは図1の各部位に相当する機能を更に詳細に示したものである。図1の説明では、伝搬推定部650は周波数・時間ずれや位相情報など様々な状態を推定するものとしたが、ここでは遅延プロファイルを推定する方法についてのみ説明する。

【0050】

伝搬推定部650は、入力バッファ601と、基準信号系列格納部602と、コンボルバ603と、出力バッファ604とからなり、符号化部651は、量子化部605と、変換部606、コードブック607とからなる。601は、入力した受信信号を一定長だけ一時保持する入力バッファであり、602は予め定められた基準信号系列を格納、順次出力する基準信号格納部であり、603は一時保持された受信信号と基準信号系列を畳み込み演算して相関値を出力するコンボ

ルバであり、604は算出された相関系列を一時保持する出力バッファである。
605はコードブック607に記録された量子化ベクトルの中から、入力されたベクトル列に最も類似したものを検索しコードを出力する。606は、量子化部605が出力するコードに対応する暗号鍵をコードブックから選択し、出力する。

【0051】

607はコードブックであり、この中には量子化ベクトルと暗号鍵が格納されている。図18は遅延プロファイルのテンプレートとなる量子化ベクトルと、それに対応する暗号鍵とが格納されたコードブックの例を示している。

以上ような構成における動作を説明する。

【0052】

まず、伝搬推定部650は、基準信号を含む受信信号を入力バッファ601に保持する。コンボルバ603は、基準信号格納部602からの基準信号系列と、入力バッファ601に保持された受信信号系列とのスライディング相関を演算した結果を相関系列として出力し、それらを順次出力バッファ604に保持する。出力バッファ604で保持された相関系列は、基準信号系列と受信信号系列との相関値、則ち遅延プロファイルに相当するデータが格納されている。これらの遅延プロファイル情報は、一連の入力ベクトルとして符号化部651へと送出される。この様にして求められる遅延プロファイル情報の一例を図16に示す。

【0053】

量子化部605は出力バッファ604からの入力ベクトルと、コードブック607の量子化ベクトルに記録されたベクトルとを照合し、類似性の最も高いものを抽出し、その対応コードを出力する。具体的には、入力ベクトルを X_{in} 、コード m の量子化ベクトルを X_{qm} ($m: 1 \sim M$) とすると、

【0054】

【数1】

$$d = |X_{in} - X_{qm}|^2$$

【0055】

が最小になる X_{qm} を求めることとなる。このようにして求めた量子化ベクトルの対応コード m を出力する。

【0056】

変換部 606 は遅延プロファイルの対応コード m と、コードブックの暗号鍵テーブルの内容とから対応する暗号鍵を出力する。このような構成で暗号鍵を決定することにより、柔軟な暗号鍵の設定が簡単な回路で実現可能になる。

【0057】

以上の説明において、符号化部 105 の遅延プロファイルの符号化方法として量子化ベクトル手法を用いる方法について説明したが、遅延プロファイルのデータ系列を評価式で近似し、それから得られる近似式の係数を利用するなどして符号化する事や、遅延プロファイルを幾つかのブロックに分割して、その大きさや、順番から符号化したり、最大パワーを有するパスの遅延時間とその大きさによって符号化したりするなど様々な方法が考えられる。

【0058】

(実施の形態 3)

伝搬制御により安定した通信方法の発明について図 4 および図 5 を用いて説明する。第 1 の実施の形態で説明した構成に類似しているため、ここでは相違点のみ説明する。

【0059】

図 4 の 401 は複数のアンテナ素子から構成されるアンテナ、453 は暗号受信部、454 は暗号送信部である。暗号受信部 453 は受信復調部 450 と、暗号鍵生成部 451 と、復号部 407 とで構成されており、図 1 の各部位と同じ構成でなっている。暗号送信部 454 は、基準信号生成部 408 と、暗号化部 409 と、切換部 410 と、送信変調部 452 とからなっており、基準信号生成部 408、暗号化部 409、切換部 410 は図 2 中の対応する部位と同じである。

【0060】

送信変調部 452 は、伝搬制御部 411 と、変調部 412 と、送信部 413 とで構成されている。411 は伝搬推定部 403 から出力される伝搬情報と、符号化部 405 が伝搬情報から特徴を抽出した伝搬特徴情報とを入力し、通信相手の

端末に対しての伝搬状態が最適になるように制御するよう、変調制御信号と、送信制御信号とを出力する伝搬制御部である。412は伝搬制御部411から出力された変調制御信号と通信情報とを入力し、変調制御信号に基づき位相や出力タイミング、振幅の微調整などを行いながら通信情報を変調し、各アンテナ素子に対応する変調信号を出力する変調部である。

【0061】

413は、送信制御信号と変調信号とを入力し、送信制御信号に基づき、周波数や出力タイミングなどを制御しながら変調信号を、各アンテナ素子に対応するRF信号へ変換しアンテナ401へと出力する送信部である。

【0062】

以上のように構成された通信装置について、図5の通信手続きを用いながらさらに詳細に説明する。図5中の基地局、端末ともに図4のように構成された通信装置として説明を行う。なお、ここでは第1の実施の形態からの相違点のみを記述する。

【0063】

(0) 基地局、端末：初期化

第1の実施の形態と同様な動作を行う。

【0064】

(1) 基地局：第1基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第1基準信号として出力する。具体的には、切換部410は基準信号生成部408で生成される基準信号を選択し、送信変調部452へ出力する。送信変調部452では選択された通信情報と、伝搬情報と伝搬特徴情報とを入力し、通信相手である端末への伝搬状態を制御しながらRF信号を出力しアンテナ401から放射する。この伝搬制御については別途詳細に説明する。

【0065】

端末は基地局からの信号を待っており、伝搬推定部403は受信した受信信号から第1基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。この推定値である伝搬情報は、符号化部405と伝搬制御部411へ送

出される。符号化部 4 0 5 は、伝搬推定部 4 0 3 からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴情報を伝搬制御部 4 1 1 へ出力する。同時に、抽出した伝搬特徴情報を用いて暗号鍵への変換を行う。変換された暗号鍵はバッファ部 4 0 6 に保持され暗号鍵情報が出力される。この暗号鍵を第 1 鍵として基地局は以降の通信の暗号鍵とする。

【 0 0 6 6 】

(2) 端末：第 2 基準信号送信

端末は、(1)と同様に基地局で行う伝搬推定用の基準信号を第 2 基準信号として出力する。この時、伝搬制御部 4 1 1 は(1)で求めた伝搬情報と、伝搬特徴情報とから、通信相手である基地局に対して暗号鍵(第 1 鍵)に対応する伝搬状態になるように変調部 4 1 2 と送信部 4 1 3 を制御しながら第 2 基準信号を送信する。

【 0 0 6 7 】

基地局では、端末からの信号を受信すると第 2 基準信号を検出し、伝搬推定部 2 0 3 は受信信号と既知信号である基準信号とから伝搬推定を行う。(1)と同様、伝搬推定部 4 0 3 は伝搬情報を出力し、符号化部 4 0 5 は伝搬情報から伝搬特徴情報を抽出して出力する。さらに伝搬特徴情報から暗号鍵へと変換され、バッファ部 4 0 6 で暗号鍵情報が保持される。この暗号鍵を第 2 鍵として端末は以降の通信の暗号鍵とする。

【 0 0 6 8 】

(3) 基地局：暗号送信

基地局は、切換部 4 1 0 の状態を、暗号化部 4 0 9 から出力される暗号化情報を選択するように切り換える。暗号化部 4 0 9 は(2)で得られた第 2 鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化情報を出力する。暗号化情報は切換部 4 1 0 で選択され、選択された通信情報が送信変調部 4 5 2 へと出力される。送信変調部 4 5 2 では、伝搬制御部 4 1 1 が(2)で求めた伝搬情報と、伝搬特徴情報とから、通信相手である端末に対して暗号鍵(第 2 鍵)に対応する伝搬状態になるように変調部 4 1 2 と送信部 4 1 3 を制御しながら RF 信号としてアンテナ 4 0 1 から暗号化信号を放射する。

【0069】

端末は、暗号化信号を受信すると受信復調部450が受信信号を復調情報へと復調する。復号化部407は復調情報と(1)で求めた第1鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

【0070】

(4) 端末：暗号送信

端末は、(3)と同様に第1鍵を用いて暗号化を行い暗号化情報を出力する。送信変調部452では、(1)や(3)で求めた伝搬情報と、(1)で選択した暗号鍵に対応する伝搬特徴情報とから、通信相手である基地局に対して暗号鍵(第1鍵)に対応する伝搬状態になるように変調部412と送信部413を制御しながらRF信号としてアンテナ401から暗号化信号を放射する。基地局は、(3)と同様に(2)で求めた第2鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

【0071】

第1の実施の形態で示したことと同様、基地局と端末が生成した暗号鍵(第1鍵および第2鍵)は共有鍵として利用が可能である。則ち、(3)や(4)における暗号化・復号化は問題なく処理されることが分かる。

【0072】

更に本方式では、送信変調部452に於いて受信時で求めた伝搬情報と暗号鍵に対応した伝搬状態を示す伝搬特徴情報とから、通信相手となる端末に対しての伝搬状態を、伝搬特徴情報になるよう制御されているため、受信時の伝搬状態と想定された(暗号鍵に対応する)伝搬状態との誤差が小さくなり、通信品質が大幅に向上するといった有利な特長を有する。

【0073】

また、伝搬状態が変化した場合でも、伝搬制御を行うことで通信の安定性を向上させることが出来る。

【0074】

また、暗号鍵を選択する際に符号化部405が検索したテンプレートの中で、類似したものが複数存在する場合、送信側が明示的に伝搬状態を制御することで

曖昧さを排除する事が出来る。

【0075】

通信手順で、基準信号を送信する際、第1基準信号の送信と第2基準信号の送信を行っているが、両者はどちらが先に実施されても本方式に影響を与えるものではないことは明白である。当然、暗号通信の手順も同様で、その順序によって本方式には影響を与えない。

【0076】

本方式では、基準信号の通信を以て暗号鍵の授受を行っており、基準信号以降の暗号化信号については、その暗号鍵と先に授受したそれとが一致していればよい。つまり、(3)や(4)において送信側が受信側に対して伝搬制御を行いつながり通信を行っているが、暗号鍵がしめす伝搬状態と一致する必要はない。

【0077】

また、通信手順の中で基準信号を別途通信しているが、これは、図9のフレーム構成(b)、(c)のように、データストリームの中に基準信号を挿入することで、(1)と(3)あるいは(2)と(4)の手順を同時に実施することができるといった有利な特長を有することが出来る。

【0078】

(実施の形態4)

通信相手である端末に対して伝搬状態を制御する方法について図6、図7を用いて説明する。また、ここでは通信端末のアンテナ401は4つのアンテナ素子(AN1~AN4)からなるものとする。

【0079】

図6における動作は、第2の実施例で記述したものと基本的には同一である。ここでは、相違点のみ説明する。

【0080】

コンボルバ603は、夫々の受信信号に対して基準信号を用いて遅延プロファイルを生成し、4種類の遅延プロファイルが出力バッファ604で保持される。ここで、各遅延プロファイルをDs1~Ds4とする。さらに、受信信号と受信重み付け係数(Wr1~Wr4)を用いて

【0081】

【数2】

$$R_0 = \sum R_m \cdot W_{rm}$$

【0082】

で与えられる受信信号 R_0 の遅延プロファイル(D_{s0})を計算し出力する。
 これらの遅延プロファイル($D_{s0} \sim D_{s4}$)のうち、 D_{s0} は符号化部651へ入力され、暗号鍵 K_0 、対応コード m_0 が出力される。
 なお、受信重み付け係数 $W_{r1} \sim W_{r4}$ は初期状態などにおいて初期値に設定されるものとする。

【0083】

このようにして求められた $D_{s1} \sim D_{s4}$ 、 $W_{r1} \sim W_{r4}$ 、 D_{s0} 、 m_0 を用いて伝搬制御を行う具体的な方法について図7を用いて説明する。

【0084】

図7の701は4つのアンテナ素子で構成されるアンテナ、702は各アンテナ素子からのRF信号を入力し、各受信信号および受信系列に対応する受信重み付け係数を出力する受信復調部、703は受信重み付け係数と各受信信号とを入力し、伝搬推定を行い伝搬情報を出力する伝搬推定部、704は伝搬情報から特徴を抽出し暗号鍵の対応コードを出力する符号化部、750は伝搬情報と暗号鍵の対応コードと、受信重み付け係数とを入力し、送信重み付け係数を出力する伝搬制御部、751は通信情報と送信重み付け係数とから各アンテナに対して送信信号を生成し出力する送信変調部である。伝搬制御部750は、係数算出部705と、コードブック706と、係数バッファ707とからなる。705は伝搬情報と暗号鍵の対応コード、受信重み付け係数、量子化ベクトルを入力して送信信号のアンテナ素子に対応する送信重み付け係数を出力する。

【0085】

706は送信重み付け係数を保持する係数バッファであり、707は対応コードと量子化ベクトルを格納したコードブックである。送信変調部751は、変調部708と、信号ウェイト部709と、送信部710とからなる。708は通信

情報を入力して所定の変調方式で変調し、変調信号を出力する変調部、709は変調信号とアンテナ素子に対応した重み付け係数とを乗じて、重み付け変調信号を出力する信号ウェイト部、710はアンテナ素子に対応する重み付け変調信号を入力し、夫々の信号をアンテナ素子に対応するRF信号を出力する送信部である。

【0086】

図7で説明した各ブロックの機能は、図4、図6に記述された各部位とほぼ同等である。ここでは、相違点のみにについて説明する。

【0087】

アンテナ701は4つのアンテナ素子(AN1~AN4)から構成されるアンテナであり、受信したRF信号をアンテナ素子毎の4系統出力する。また受信時に用いるアンテナ毎の受信重み付け係数(Wr1~Wr4)も同時に出力する。AN1~AN4に対応する受信信号(R1~R4)は伝搬推定部703に入力される。上述の通り、伝搬推定部703では各受信信号(R1~R4)に対応する伝搬状態(Ds1~Ds4)を出力し、符号化部704は暗号鍵K0、対応コードm0を出力する。

【0088】

係数算出部705は、暗号鍵K0に対応するコードm0をコードブック706で検索し、コードm0の対象となっている量子化ベクトル(Xqm0)を読み、保持する。量子化ベクトル(Xqm0)と入力された伝搬情報(Ds0~Ds4)とを用いて

【0089】

【数3】

$$d = |W_m \cdot D_{s m} - X_{q m 0}|^2$$

【0090】

で与えられる2乗誤差が最小になるようなWm(m:1~4)を求める。この算法としては最小2乗法などが有名である。

【0091】

こうして得られた重み付け係数 ($W_1 \sim W_4$) と受信重み付け係数 ($W_{r1} \sim W_{r4}$) とを用いて

【0092】

【数4】

$$W_{tm} = W_m / W_{rm} \quad (m: 1 \sim 4)$$

【0093】

で与えられる送信重み付け係数 ($W_{t1} \sim W_{t4}$) を求め出力する。係数バッファ706は送信重み付け係数を保持する。

一方、通信情報を入力した変調部708は、所定の変調方式に従って通信情報を変調し、変調信号を出力する。この変調信号は、アンテナ素子 ($AN_1 \sim AN_4$) に対応する変調信号系統 ($S_1 \sim S_4$) に分岐され、信号ウェイト部709へ送出される。信号ウェイト部709では、係数バッファ706からの送信重み付け係数 ($W_{t1} \sim W_{t4}$) と、 $AN_1 \sim 4$ に対応した変調信号 ($S_1 \sim S_4$) とを乗じる。

【0094】

【数5】

$$S_{wm} = W_{tm} \cdot S_m \quad (m: 1 \sim 4)$$

【0095】

こうして得られた重み付け変調信号 ($S_{w1} \sim S_{w4}$) を出力する。送信部710は、重み付け変調信号を入力し夫々をRF信号 ($S_{rf1} \sim S_{rf4}$) に変換してアンテナ701へ出力する。

【0096】

以上のような計算を行いながら送信変調部751において送信重み付け係数を乗ずることで、受信する端末において X_{qm0} で表される伝搬特性に制御が可能となる。

【0097】

以上の説明では、遅延プロファイルを制御するものとして説明したが、これは

偏波状態（偏波面、旋回方向）や、位相状態、伝搬遅延時間についても同じ事がいえる。

【0098】

ここで、コードブック706は符号化部704が持っているコードブックと同一のものであり、構成上はどちらか一方が在ればよい。

【0099】

また、アンテナ701はアンテナ素子数が4の場合について説明したが、4に限らず2以上であれば同様の効果が得られることはいうまでもない。

【0100】

また、数式で示した各符号は自然数であっても、複素数であっても適用可能である。各値が複素数である場合、信号制御が振幅と位相で行えるため、より高度な制御を期待できる。

【0101】

（実施の形態5）

伝搬制御を行うことで、任意の暗号鍵を選択できる方法について図4、図9を用いて説明する。

【0102】

上述の方法では、推定した伝搬状態に対応する暗号鍵を選択して通信を行うことから、伝搬状態が一定である場合、暗号鍵が長時間の間同一となってしまう。そのため、暗号鍵の推定が容易になってしまう虞がある。また、両通信装置で同一の暗号鍵を用いるため、一方の暗号鍵が判明した場合、他方の暗号鍵も判明してしまうといった虞がある。ここでは、第4の実施の形態で示した伝搬制御の方式を用いることで、送信側が暗号鍵を制御し前述の問題を解決する手段について説明する。

【0103】

図9は、本発明に関する通信手順を示したものである。図中の（0）～（4）の手順は、図5で示した手順と同一であるが、上述の方式では第1鍵と第2鍵が同一であったものに対して、これを送信者が選択できるところが異なる。ここでは、（5）以降を説明する。また、図4の装置を用いて動作説明をしている。

【0104】

(5) 基地局：第3基準信号送信

基地局は、暗号鍵として第3鍵を選択しその暗号鍵に対応する伝搬特徴情報と、最後に推定された通信の伝搬情報とから重み付け係数を決定する。次に、端末で行う伝搬推定用の基準信号を重み付け係数によって伝搬制御を行いながら第3基準信号として出力する。

【0105】

端末は基地局からの信号を待っており、伝搬推定部403は受信した受信信号から第3基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。この推定値である伝搬情報は、符号化部405と伝搬制御部411へ送出される。符号化部405は、伝搬推定部403からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴情報を伝搬制御部411へ出力する。同時に、抽出した伝搬特徴情報を用いて暗号鍵への変換を行う。変換された暗号鍵はバッファ部406に保持され暗号鍵情報が出力される。この暗号鍵を第3鍵として基地局は以降の通信の暗号鍵とする。

【0106】

(6) 端末：第4基準信号送信

端末は、(5)と同様に暗号鍵として第4鍵を選択しその暗号鍵に対応する伝搬特徴情報と、最後に推定された通信の伝搬情報とから重み付け係数を決定する。次に、基地局で行う伝搬推定用の基準信号を重み付け係数によって伝搬制御を行いながら第4基準信号として出力する。

【0107】

基地局では、端末からの信号を受信すると第4基準信号を検出し、伝搬推定部403は受信信号と既知信号である基準信号とから伝搬推定を行う。(5)と同様、伝搬推定部403は伝搬情報を出力し、符号化部405は伝搬情報から伝搬特徴情報を抽出して出力する。さらに伝搬特徴情報から暗号鍵へと変換され、バッファ部406で暗号鍵情報が保持される。この暗号鍵を第4鍵として端末は以降の通信の暗号鍵とする。

【0108】

(7) 基地局：暗号送信

基地局は、(5) で選択した第3鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化信号を送信する。

【0109】

端末は、暗号化信号を受信すると受信復調部450が受信信号を復調情報へと復調する。復号化部407は復調情報と(5)で求めた第3鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

【0110】

(8) 端末：暗号送信

端末は、(6) で選択した第4鍵を用いてセキュリティデータを暗号化し、暗号化信号を送信する。

【0111】

基地局は、(7)と同様に(6)で求めた第4鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

【0112】

以上の動作について数式を交えて説明する。

【0113】

電波伝搬の特性を表す伝搬関数 H 、受信信号 S_r 送信信号 S_t を用いて表すと

【0114】

【数6】

$$S_r = H \cdot S_t$$

【0115】

の式が成り立つ。アンテナの素子数を N とすると、 H は $N \times N$ の正方行列、 S_r と S_t は $1 \times N$ の行列である。端末は基地局が送信する信号(図3では第1基準信号)、基地局は端末が送信する信号(図3では第2基準信号)を用いて計算することができる。第1基準信号および第2基準信号の通信を式で表すと

【0116】

【数 7】

$$S r_b = H u \cdot S t_m$$

$$S r_m = H d \cdot S t_b$$

【0117】

と表現できる。HuおよびHdはアップリンク・ダウンリンクの伝搬関数、St__b、Sr__bは基地局側の送受信信号、St__m、Sr__mは端末側の送受信信号である。また、St__bおよびSt__mは既知信号（第1、第2基準信号）であるから、伝搬関数はそれぞれ

【0118】

【数 8】

$$H u = S r_b \cdot S t_m^{-1}$$

$$H d = S r_m \cdot S t_b^{-1}$$

【0119】

で求められる。伝搬関数は伝搬の相反性から、送信時と受信時では同一となることから、

【0120】

【数 9】

$$H \equiv H u = H d$$

【0121】

である。この様にして得られた伝搬関数Hを暗号鍵（第1鍵（=第2））に用いるのが第1の実施の形態に示したものである。

【0122】

一方、送信重み付け係数Wb、Wmを用いて伝搬状態を制御する方法について説明する。暗号鍵（第1鍵（=第2鍵））を選択する際に求めた量子化ベクトルで示される伝搬関数H' と実際の伝搬関数Hとの間に誤差εがある場合は、

【0123】

【数10】

$$S_r = (H' \cdot \varepsilon) \cdot S_t$$

【0124】

で示されるから、誤差成分 ε は

【0125】

【数11】

$$\varepsilon = H^{-1} \cdot (S_r \cdot S_t^{-1})$$

【0126】

で求めることができる。これを重み付け係数 W_m 、 W_b に置き換えることで

【0127】

【数12】

$$S_{r_b} = (H' \cdot W_m) \cdot S_{t_m}$$

$$S_{r_m} = (H' \cdot W_b) \cdot S_{t_b}$$

【0128】

のように補正が可能である。この様にして重み付け係数を用いて伝搬状態を補正しながら暗号通信を行うのが第4の実施の形態に示したものである。さて、この補正機能をさらに発展することで、暗号鍵を送信側で設定することも可能である。第1鍵(=第2鍵)とは異なる第3鍵、第4鍵を用いる場合について説明する。基地局は、第3鍵に対応する伝搬関数 H_3 になるよう重み付け係数 W_{3_b} によって制御を行い、これを第3基準信号を通じて送信する。すなわち、

【0129】

【数13】

$$S_{r_m} = (H \cdot W_{3_b}) \cdot S_{t_b}$$

【0130】

とした場合、

【 0 1 3 1 】

【数 1 4】

$$H3 = H \cdot W3_b$$

【 0 1 3 2 】

である。以降基地局は第 3 鍵を用いて暗号化を行いながら暗号化通信を実施する。

端末は、第 3 基準信号を受信し伝搬状態を解析することで、伝搬関数 $H3$ を得ることが出来るからそれに対応する暗号鍵（第 3 鍵）を用いて、以降の暗号化情報を復号していけばよい。同様にして、端末側は第 4 鍵を選択（対応する伝搬関数は $H4$ とする）し、重み付け係数 $W4_m$ によって制御を行いながら第 4 基準信号を通じて送信する。

【 0 1 3 3 】

【数 1 5】

$$S r_b = (H \cdot W4_m) \cdot S t_m$$

$$H4 = H \cdot W4_m$$

【 0 1 3 4 】

端末は第 4 鍵を用いて暗号化を行いながら暗号化通信を実施する。同様にして基地局が第 4 鍵を用いて復号可能である。

【 0 1 3 5 】

（実施の形態 6）

基準信号と暗号化信号の通信手順について図 8、図 9、図 10 を用いて説明する。

【 0 1 3 6 】

他の実施の形態において説明したフレーム構成は図 9 の（a）を基準に説明してある。つまり、基準信号を含むバーストと、暗号化信号を含むバーストが別に存在している形態である。この方式を用いると基準信号期間を長く取れるため、受信側の推定誤差を小さくできるといった特長がある。

【 0 1 3 7 】

一方、フレーム構成 (b) は、データストリーム (或いはバースト) 中に所定の期間、基準信号を挿入する方法である。この方式によると、暗号化信号と同時に暗号鍵を授受することが可能であり、効率的な伝送を行うことが出来るようになる。

【 0 1 3 8 】

フレーム構成 (c) は、同 (a)、(b) とは異なり、基準信号が示す暗号鍵と暗号化信号が用いる暗号鍵の配置について示している。図に示すように、基準信号が示す暗号鍵と対応するデータ信号との間で時間的 (或いは周波数的) に所定の方式に従って変化を付けることで、暗号鍵と対応する暗号化信号とを独立して授受することが可能となるため、第 3 者へ両者が漏洩する危険性が減るといった特長を有する。

【 0 1 3 9 】

暗号鍵の授受については、他の実施の形態において通信手順にも示した通り、基準信号を用いて行われていることとしている。図 8 の (1)、(2)、(5)、(6) がそれに相当する。図 8 では、これ以外の通信では暗号鍵の授受は行われていない。これは、暗号化通信時の伝搬状況には復号動作が左右されないことを示している。つまり、基準信号の送信時は伝搬環境に応じて特徴的な伝搬情報が伝達できるように伝搬制御を行うことで安定した暗号鍵の授受が可能となる。

【 0 1 4 0 】

図 1 0 を用いて説明する。図 1 0 は通信手順と対応する伝搬制御の操作を示す図である。

【 0 1 4 1 】

まず、図 9 のフレーム構成 (a) における通信について説明する。

【 0 1 4 2 】

(1 a) において基準信号が送信される際、伝搬制御は他の実施の形態で述べたように暗号鍵を授受するための通信を行う。この時、以前に伝搬推定を実施していれば、その推定結果と暗号鍵に対応する伝搬状態との差を補正するような制御を行うことが可能である。こうすることで受信側は伝搬状態が良好な状態で基

準信号を受信可能であり、安定した暗号鍵授受が行えることになる。一方、(2 a)において、データ通信(暗号化信号)を行う場合、暗号鍵は既に受信側に届いており、受信・復号に伝搬情報を用いる必要はない。このため、制御方式としては受信が安定して行えるような制御(ビームフォーミング、送信側の等化、送信ダイバーシチなどが知られている)を行うことでデータ通信を安定して行うことが出来る。以降、(3 a)～(5 a)・・・の様に通信を行うことで大幅な通信品質の向上が見込める。

【0 1 4 3】

次に、図9のフレーム構成(b)における通信について説明する。

【0 1 4 4】

図10の(1 b)に示すように、基準信号通信時とデータ通信時とで伝搬制御方式を切り換えることが考えられる。この方式を用いると、暗号鍵と暗号化信号とを同時に伝達することが可能である。送信側で暗号を選択できることは既述の通りであるが、その特性を利用することで毎ブロック暗号鍵を変更するといった柔軟な事も可能になる。その上、先に説明したように安定した通信が行えるといった特長がある。

【0 1 4 5】

一方、基準信号通信時とデータ通信時の伝搬制御方式を同一にすることも当然可能である。この場合、データ通信時の復調に基準信号を利用することが可能となり、通信品質の向上が見込める。

【0 1 4 6】

以上、説明の中で基準信号として既知信号を想定して説明を行った。しかし、基準信号は既知信号である必要はない。この場合、復調しながら伝搬の変化を推定し、暗号鍵を決定する事になる。このようにする事で、暗号鍵を決定するための情報が増加し、安定して暗号鍵の検出が行えるようになる。また、基準信号はQAM変調などに用いられるパイロット信号、TDMAなどで行うバースト同期用の同期信号系列などを用いることも可能であり、このような構成によると、従来構成をほとんど変更せずに高いセキュリティ性を確保した通信が提供できるといった特長がある。

【0147】

(実施の形態7)

ここでは、多重した信号への適用方法について図11、図12を用いて説明する。多重アクセス方式としてはCDMAを例に挙げる。

【0148】

図11は本発明に供する受信装置の一部を示したものである。

【0149】

1150は受信復調部であり、RF信号を受信した受信信号と復調した復調情報とを出力する。1150は受信部1101、逆拡散部1102、伝搬推定部1103、復調部1104とからなる。

【0150】

1101は受信部、1102は受信信号とチャネルに対応する拡散符号との畳み込み積分を行い逆拡散信号を出力する逆拡散部、1103は各チャネルの伝搬推定をおこない各チャネルに対しての伝搬情報を出力する伝搬推定部、1104は復調部、1105はチャネル毎の伝搬情報を比較し比較結果を出力する比較部、1151は暗号鍵生成部、1106は復号化部である。

【0151】

図12は本発明に供する送信装置の一部を示したものである。

【0152】

1201はチャネル毎のデータを保持する第1データバッファ、1202はチャネル毎のデータを変調しチャネルに対応する拡散符号で拡散して、拡散信号を出力する変調拡散部、1203は暗号鍵を一時保持する暗号鍵バッファ、1204は第2データを格納する第2データバッファ、1205は伝搬状態の基準情報を保持する基準伝搬バッファ、1206は暗号鍵と第2データと伝搬情報とを入力し送信重み付け係数を算出する伝搬制御部、1207は送信信号と送信重み付け係数を乗ずる送信ウェイト部、1208は送信部である。

【0153】

以上の構成による動作について詳細に説明する。

【0154】

送信装置は、第1データバッファ1201から複数チャネル分のデータを取りだし夫々を変調し、予め設定されている拡散符号を用いて各チャネルの拡散信号を生成する。暗号鍵バッファ1203と第2データバッファ1204はそれぞれ暗号鍵と第2データを出力し、それを入力した伝搬制御部1206は、事前に推定された伝搬情報が保持された基準伝搬バッファ1205からの情報を基に、第2データ、暗号鍵に対応する伝搬状態制御を、送信重み付け係数によって行う。送信重み付け係数は送信ウェイト部1207で重み付け演算が行われ、送信部1208を通じて送信される。

【0155】

まず、簡単のため第2データバッファ1204からの出力がないものとする。伝搬制御1206の制御自体は第5の実施の形態で示したものと同一である。例えば、チャネルが1つである場合は第4の実施の形態でしめした基準信号を出力している状態と一致する。チャネルが複数ある場合を考える。拡散符号はチャネル毎に設定されているが、各符号間の相関はないため、信号処理上ではそれぞれが独立に処理されていることと同義となる。則ち、伝搬制御部1206はチャネル数をM、アンテナ数をNとすると $M \times N$ 個以上の送信重み付け係数によってチャネル毎に伝搬制御が行えることになる。

【0156】

以上説明した通り、第5の実施の形態同様に暗号鍵に応じた伝搬制御が行えることが分かる。

【0157】

さて、複数チャネルが多重されている場合、チャネル毎に伝搬制御を行うことにより、受信端での受信電力を制御することも可能である。例えば、暗号鍵の状態に応じて、どのチャネルが最大電力とするかを制御できることになり、このチャネル番号と受信電力の関係によって受信装置は暗号鍵を決定することが可能となる。さらに、上述のとおり、伝搬パラメータとして（例えば遅延プロファイル）を設定できるので、例えば遅延プロファイルに暗号鍵情報を、チャネルと受信電力の関係に第2データを利用すること（或いは逆でも構わないし、暗号鍵情報だけ、第2データだけといったことも可能である）によって、より多くのセキュ

アな情報を送信することが可能であることがわかる。

【0158】

さらに、第1データバッファ1201に格納されたデータのうち、1つを基準信号とすることも可能である。この様にすることで、受信装置は第1データや第2データと同時刻に基準信号による伝搬推定の実施が可能になるので、非常に効率の高い伝送が可能になるといった特長を有する。

【0159】

次に、受信処理について説明する。

【0160】

伝搬パラメータ（遅延プロファイルなど）を用いて暗号鍵情報を授受する方法については、逆拡散処理を除き上述のものと同一に行うことが可能である。ここでは、多重化されたチャネルと受信電力の關係に情報が重畳されている場合についてのみ説明を行う。

【0161】

アンテナから入力されたRF信号は受信部1101で受信され受信信号が出力される。受信信号は逆拡散部1102において、チャネル毎に予め設定された拡散符号とで畳み込み演算が施され、逆拡散信号がチャネル数分出力される。これら逆拡散信号は、伝搬推定部1103へ入力され伝搬状態が推定される。ここでは伝搬状態のうち、受信電力を用いるものとする。伝搬推定部1103からチャネル毎の受信電力が出力されると、比較部1105によって受信電力の比較が行われ、この結果を暗号鍵情報（或いは第2データ）として出力する。

【0162】

この様にして決定された暗号鍵を用いて、復号化部1106は以降の復調情報を復号化し、セキュリティデータを得る。

【0163】

以上の説明では、CDMAを例に挙げたがOFDMでも同様の効果が得られることはいうまでもない。OFDMとなる場合、上記説明におけるチャネルをサブキャリアとし、図11の逆拡散部処理はフーリエ変換処理に、図12の拡散処理は逆フーリエ変換処理に置き換えることで可能である。

【0164】

(実施の形態8)

第4の実施の形態で用いる伝搬情報として遅延プロファイルに変えて受信到来方向情報を利用した方式について説明する。ここでは相違点のみについて図7、図8、図13を用いて説明する。

【0165】

到来方向推定を行う際の構成を、図4の伝搬推定部403および、符号化部405の詳細ブロック図を図13に示す。

【0166】

伝搬推定部1350は、入力バッファ1301、相関行列演算部1302、行列演算部1303、角度スペクトラム演算部1304、出力バッファ1305で構成されており、1306は送信側の放射方向と受信信号到来方向との対比データを格納し夫々を変換する参照テーブルである。

【0167】

1301は、入力信号を一時保持する入力バッファ、1302は入力信号の相関行列を求める相関行列演算部、1303は計算された相関行列を入力し行列演算（ここでは固有ベクトル）で求めた固有ベクトルを出力する行列演算部、1304は、固有ベクトルを入力して角度スペクトラム演算し到来方向推定情報を出力する角度スペクトラム演算部、1305は演算結果を一時保持する出力バッファである。また、到来方向を伝搬情報として用いる場合は、図18に示したコードブックの量子化ベクトルは到来方向情報の内容が記述されている。

【0168】

以上の構成は到来方向推定法として知られているMUSIC法を用いている。他に、フーリエ法やCAME法が知られているが、これは行列演算部1303の演算内容によって分類される。

【0169】

以上の構成において、伝搬推定部1350が伝搬情報として到来方向推定を行う際の動作について詳細に説明する。

【0170】

複数のアンテナ素子から入力された受信信号は、入力バッファ1301において保持される。保持された受信信号は相関行列演算部1302においてその相関行列が求められ、次に行列演算部1303において固有ベクトルが算出される。角度スペクトラム演算部1304は固有ベクトルから、受信信号到来パターン情報を算出しこれを出力する。この様にして得られた受信信号到来パターン情報は出力バッファ1305で保持される。この様にして求められる受信信号の到来方向情報の一例を図17に示す。図17では信号の到来方向が2つ存在する場合の推定結果を示している。

【0171】

この様にして得られた受信信号の到来パターン情報を用いて、図8の手順で説明を行う。ここでも相違点のみ述べる。

【0172】

(1) 基地局：第1基準信号送信

基地局は、端末の伝搬推定用に第1基準信号を送信する。この時、複数のアンテナ素子によるビームステアリングを行って、放射パターンを変化させながら送信する。

【0173】

端末は、基地局が出力する基準信号を検出すると、伝搬推定部1350は、到来方向推定を行い、基地局が制御する放射方向と、端末における受信信号到来パターン情報との対比データを参照テーブル上に格納する。以上の操作により、基地局と端末との間における放射パターンと受信到来パターンとの参照テーブルができあがる。

【0174】

(2) 端末：第2基準信号送信

端末は、暗号鍵（第1鍵）を選択し、コードブックからそれに対応する到来方向情報を出力する。この到来方向情報を、参照テーブルに格納されている放射パターンに最も類似しているものを検出し、これに対応する到来パターン情報を出力時の放射パターンとして設定する。次に、基地局の伝搬推定用に第2基準信号を、設定した放射パターンになるよう制御しながら送信する。

基地局は、伝搬推定部 1350 で到来方向推定を行い受信到来パターンを出力する。符号化部 405 は受信到来パターンとコードブックから暗号鍵（第 2 鍵）を選択し、バッファ 406 を介して復号化部 407 へ出力する。

【0175】

（3）基地局：暗号化信号送信

基地局は、（2）で求めた受信到来パターンから、端末の受信状態が良好になるような放射パターンに設定する。次に第 2 鍵を用いてセキュリティデータを暗号化し、設定した放射パターンになるよう制御しながら暗号化信号を送信する。端末は、RF 信号を受信復調部 450 で復調し、復号化部 407 で第 1 鍵を用いて復号化し、セキュリティデータを出力する。

【0176】

（4）端末：暗号化信号送信

端末は、（1）で求めた受信到来パターンから、基地局の受信状態が良好になるような放射パターンに設定する。次に、セキュリティデータを第 1 鍵で暗号化させながら設定した放射パターンになるように制御しながら暗号化信号を送信する。

基地局は、RF 信号を受信復調部 450 で復調し、復号化部 407 で第 2 鍵を用いて復号化し、セキュリティデータを出力する。

【0177】

以上のように通信を行うことで、第 3 者に到達する受信到来パターンは大きく変化するため、非常に高いセキュリティを確保出来る。さらに、上述したような遅延プロファイルによる方式を組み合わせることで、一層高いセキュリティが期待できるといった特長を有する。

【0178】

また、受信信号の到来方向に情報を重畳することや、到来方向に対して通信の多重化を行うことも可能である。

【0179】

通信手順はここで説明したものに限られるものではない事は、他の実施の形態で述べたことと同じである。

【0180】

(実施の形態9)

ここでは、偏波を応用したセキュリティ通信方式について説明する。

通信方式自体は、第4の実施の形態で説明したものに類似している。ここでは相違点について図14、図15と図8を用いて説明する。

【0181】

ここで、1454は垂直偏波アンテナ1401と水平偏波アンテナ1402からなるアンテナ部であり、1450は受信復調部、1451は、位相差検出部1403と電界強度検出部1404と偏波推定部1405からなる伝搬推定部であり、1406は符号化部、1452は係数算出部1407とコードブック1408とバッファ1409からなる偏波制御部であり、1453は変調部1410と送信ウェイト部1411と送信部1412とからなる送信変調部である。受信復調部1450、符号化部1406、送信変調部1453は図7に示した対応する部位と同一である。

【0182】

1401は垂直偏波成分を受信する垂直偏波アンテナ、1402は水平偏波成分を受信する水平偏波アンテナ、1403は両偏波受信信号から位相差を検出する位相差検出部であり、1404は垂直偏波受信信号と水平偏波受信信号とから夫々の電界強度を検出する電界強度検出部であり、1405は位相差と電界強度から偏波状態を推定する偏波推定部である。1407は伝搬情報とコードブックで示される偏波コードとを入力し垂直偏波送信信号と水平偏波送信信号との位相差制御と電界強度制御を行って送信信号の偏波制御を行う係数を算出する係数算出部であり、1408はコードブック、1409はバッファである。

【0183】

以上のように構成された装置における動作について説明する。

垂直偏波アンテナ1401と水平偏波アンテナ1402は受信信号の各偏波成分を選択的に受信し、RF信号を受信復調部1450へ送出する。受信復調部1450は各偏波に対応する受信信号を出力し、これら受信信号は伝搬推定部1451へ入力される。伝搬推定部1451では、位相差検出部1403と電界強度検

出部 1404 から出力される受信位相差情報と受信電界強度情報が偏波推定部 1405 に入力され、受信信号の偏波情報が出力される。

【0184】

図 15 に偏波状態の具体例を示す。E_v が垂直偏波の電界強度、E_h が水平偏波の電界強度、p が旋回方向、 Θ が長軸角度を表している。

【0185】

このようにして求められた偏波情報は符号化部 1406 によって偏波コードに符号化され、暗号鍵が選択される。この偏波コードは偏波制御部 1452 に入力される。偏波制御部 1452 では、計数算出部 1407 がコードブック 1408 から偏波コードに対応する偏波状態を検索し、位相制御や電界強度制御などを行いながら送信重み付け係数を算出し、バッファ 1409 に保持する。バッファに保持された送信重み付け係数は、送信変調部 1453 によって垂直偏波送信信号と水平送信偏波信号とがそれぞれ重み付けされ、RF 信号として対応するアンテナ素子から出力される。

【0186】

なお、コードブック 1408 の量子化ベクトルの内容としては、偏波状態（偏波面や旋回方向など）に対応するものが格納されているものとする。通信手順については、他の実施の形態で示したものとほぼ同じである。遅延プロフィールの検出、あるいは伝搬制御の箇所が、夫々偏波情報や偏波制御に置き換わるものである。

【0187】

以上のような操作を行うことで、例えば垂直偏波、水平偏波であるとか、長軸の角度、偏波間の位相、旋回方向などが暗号鍵として用いることが可能となる。伝搬状態のなかで、偏波はアンテナに依ってのみ分離されるという特長がある。これは、他の受信装置が電波を傍受したとしても、アンテナが対応してなくてはならないことを意味し、高いセキュリティが期待できるといった特長を有する。

【0188】

また、伝搬状態として遅延プロフィールや受信パワー、到来方向パターンなどと併用することも可能である。

【0189】

(実施の形態10)

第1から第6の実施の形態を用いた方式に加え、受信端末における通信状態を制御し、その制御状態に対して情報を重畳させる方式を用いて、第3者における傍受を原理的に不可能にする方式について説明を行う。

【0190】

第5の実施の形態において、受信側における伝搬状態を任意に制御できることを示したが、この方式を用いることで物理的に秘匿性のある通信が可能になる。このことを簡単に説明する。

【0191】

上述した第5の例では、送信信号の重み付け係数によって伝搬状態を制御できることを示した。このことは、受信側に対して任意の受信状態を伝達していることと同義であり、則ち伝搬パラメータを通じて通信が行えることを意味する。換言すれば、図18に示すようなコードブックの内容（図中では暗号鍵となっているもの）を情報に置き換えることで、伝搬パラメータを通して通信が可能になることを示唆する。

【0192】

この方法を用いた通信は、別途説明したとおり通信者間で形成される伝搬環境をベースとした通信であるため、原理的に物理的位置が異なる装置に対しては高い秘匿性を有するといった特長がある。また、逆に伝搬パラメータを利用することで、伝搬経路すなわち通信相手の場所を特定していることになり、通信相手の特定や認証にも応用可能である。

【0193】

また、従来利用されてきた、変調方式（ASM、FSK、PSK、QAMなど）に依らず適用可能であり、この場合純粋にデータ容量の増加が見込める。

【0194】

さらに、多重化方式（TDMA、FDMA、CDMA、OFDMなど）などの縦断に依らず適用可能であるといった大きな特長を有する。本方式は、空間の直交性を利用した多重化も可能である。つまり、空間直交性による多重化方式と上

記多重化方式を組み合わせることで、従来のチャネル要領を大幅に増加させることが出来るといった効果も期待できる。

【0195】

また、他の実施の形態で示した暗号化、復号化の処理は特にそれを必要としない装置であれば、必須のものではなくそれがなくても動作することは明白である。

また、他の実施の形態で示した手順の中で暗号鍵情報を送信する必要がある際は、伝搬制御を通信に最適に制御（例えばマルチパス成分を除去したり、受信電力が最大になるよう制御したり）することで通信品質の向上が見込める。

【0196】

さらに、受信時においても受信信号が受信重み付け係数を用いて最適に制御（上記と同様）する事で、同様に通信品質の向上が見込める。

【0197】

（実施の形態11）

伝搬パラメータを符号化・復号化のパラメータとして用い、通信品質を向上させる方式について図19から図22を用いて説明する。

図20は送信装置の一部の説明図である。

【0198】

2050は受信したRF信号を入力し、伝搬状態を推定した伝搬情報と、復調した復調情報とを出力する受信復調部であり、図1に示した受信復調部150と同一である。2004は伝搬情報を入力しその特徴を抽出しその伝搬特徴符号を出力する伝搬情報符号化部であり、2011は伝搬状態を入力した伝搬特徴符号に近づけるよう制御する送信重み付け係数を出力する伝搬制御部であり、2051はデータを入力し、符号化（エンコード）し、情報の除去（パンクチャ）、順序変換（インタリーブ）した符号化情報を出力する符号化部であり、データを入力し畳み込み符号を出力するエンコーダ2005と、畳み込み符号を入力しその符号の一部を除去したパンクチャ符号を出力するパンクチャ部2006と、パンクチャ符号の順序を所定の順に並べ替え符号化情報を出力するインタリーブ部2007とからなる。2052は符号化情報を入力し、変調して伝搬制御し送信す

る R F 信号を出力する送信変調部であり、符号化情報を入力し所定の変調を施し変調信号を出力する変調部 2 0 0 7 と、変調信号を入力し重み付け係数を乗ずることで伝搬制御を行う送信ウェイト部 2 0 0 8 と、送信ウェイト信号を入力し送信する R F 信号を出力する送信部 2 0 0 9 とからなる。

【 0 1 9 9 】

図 1 9 は受信装置の一部の説明図である。

【 0 2 0 0 】

1 9 5 0 は受信した R F 信号を入力し推定した伝搬情報と復調した復調信号を出力する受信復調部であり、図 1 に示した受信復調部 1 5 0 と同一である。1 9 0 4 は伝搬情報を入力しその特徴を抽出しその伝搬特徴符号を出力する伝搬情報符号化部であり、1 9 5 1 は伝搬情報の特徴を示す符号と復調信号とを入力し、伝搬特徴符号に対応するインタリーブパターンを用いて順序の逆変換（デインタリーブ）、ヌル情報の追加（デパンクチャ）、復号化（デコード）し、データを出力する復号部であり、復調信号を入力し伝搬特徴符号に対応するインタリーブパターンに基づきデータ順序の逆変換を行うデインタリーバ 1 9 0 5 と、デインタリーブ信号を入力し伝搬特徴符号に対応するパンクチャパターンに基づき除去された箇所の信号に対して（後段のデコーダにとって符号を判断するのに）中立な情報を付加するデパンクチャ 1 9 0 6 と、デパンクチャ信号を入力し伝搬特徴符号に対応する畳み込み符号に対応して復号化するデコーダ 1 9 0 7 とからなる。

以上のように構成された装置と図 2 2 で示した通信手順を用いながら詳細な説明を行う。ここでは便宜上、送信装置と受信装置を組み合わせた送受装置が図 2 2 中の基地局、端末であるものとして説明を行う。

【 0 2 0 1 】

基本的な動作は第 1 の実施の形態に示したものに類似しているため、ここでは相違点のみについて説明する。

【 0 2 0 2 】

まず、予め伝搬状態に対応するインタリーブパターンや、パンクチャパターン、エンコードパターンを用意しておき、基地局、端末でこの情報を共有しておく

次に、端末は基地局が送信する基準信号により伝搬状態を推定し、これに基づく各種パターンを設定する。基地局も同様に端末から送信される基準信号により伝搬状態を推定し各種パターンを設定する。この時、設定されるインタリーブパターン、パンクチャパターン、エンコードパターンが基地局、端末と同一のものが選択されることは前述の通りである。

【 0 2 0 3 】

以上の様にして、両者の符号化パターンが設定されると次に両者の間で通信を開始する。基地局は、符号化パターンに基づきエンコーダ 2 0 0 5 によって畳み込み符号化が行われ、パンクチャ 2 0 0 6 によってパンクチャリングが行われ、インタリーブ 2 0 0 7 によってインタリーブリングが行われ、こうして得られた符号化情報が送信変調部 2 0 5 2 へ送出され、伝搬情報符号化部 2 0 0 4 が出力する伝搬特徴符号は、伝搬制御部 2 0 1 1 に入力され送信重み付け係数が出力され、送信部 2 0 1 0 によって R F 信号が出力、放射される。送信重み付け係数の算出については、第 5 の実施の形態で示したようなものと同一である。

【 0 2 0 4 】

端末では、基地局からの信号を受信し、これを受信復調部 1 9 5 0 が受信し、伝搬推定、復調を行い、伝搬情報と復調信号を出力する。復号部 1 9 5 1 では入力された伝搬特徴符号に基づき、インタリーブパターン、パンクチャパターン、エンコードパターンが選択されている。復号部 1 9 5 1 は、伝搬特徴符号と、復調信号とを入力し、デインタリーブ 1 9 0 5 では対応するインタリーブパターンの逆に対応した順序逆変換（デインタリーブリング）を行い、デインタリーブ信号を出力する。デインタリーブ信号はデパンクチャ 1 9 0 6 に入力されパンクチャパターンに対応する箇所にもル信号（後段にあるデコードの際、判断に中立な値）を挿入（デパンクチャリング）したデパンクチャ信号を出力する。デパンクチャ信号はデコーダ 1 9 0 7 に入力されエンコードパターンに基づき復号（デコード）を行い、データを出力する。

【 0 2 0 5 】

送信側と受信側において各種符号化パターンを共有していることは前述の通り

であり、このため基地局が送信するデータは端末で正常に伝送されることが分かる。

【0206】

(0) は第1の実施の形態と同一の操作である。

【0207】

(1) 基地局：第1基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第1基準信号として出力する。端末では、基地局からの信号を待っており、伝搬推定部1902は受信した受信信号から第1基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。伝搬情報符号化部1904は、伝搬推定部1902からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴符号を出力する。デインタリーバ1905、デパンクチャ1906、デコーダ1907はそれぞれ伝搬特徴符号とインタリーブパターンのテーブル、パンクチャパターンのテーブル、エンコードパターンのテーブルを持っており、入力された伝搬特徴符号から対応する各種パターン（符号化パターン）を選択する。

【0208】

(2) 端末：第2基準信号送信

端末は、(1)と同様に基地局で行う伝搬推定用の基準信号を第2基準信号として出力する。

【0209】

基地局では、端末からの信号を受信すると第2基準信号を検出し、伝搬推定部1902は受信信号と既知信号である基準信号とから伝搬推定を行う。(1)と同様、伝搬推定部1902が出力する伝搬情報は、伝搬情報符号化部1904によって伝搬特徴符号へと変換され、復号部1951で伝搬特徴符号に対応した符号化パターンが選択される。

【0210】

(3) 基地局：符号化信号送信

基地局において、符号部2051は(2)で得られた符号化パラメータを用いてデータのエンコード、パンクチャ、インタリーブした符号化情報を出力する。

符号化情報は送信変調部 2 0 5 2 へと出力され、それらを変調部 2 0 0 8、送信ウェイト部 2 0 0 9、送信部 2 0 1 0 を通じて R F 信号が符号化信号として出力される。

【 0 2 1 1 】

端末は、符号化信号を受信すると受信復調部 1 9 5 0 が受信部 1 9 0 1、復調部 1 9 0 2 を通じて R F 信号を復調信号へと復調する。復号部 1 9 5 1 は復調信号と (1) で求めた符号化パラメータを用い、デインタリーブ、デパンクチャ、デコードの順に復号を行い、データを出力する。

【 0 2 1 2 】

(4) 端末：符号化信号送信

端末において、符号部 2 0 5 1 は (1) で得られた符号化パラメータを用いてデータのエンコード、パンクチャ、インタリーブした符号化情報を出力する。符号化情報は送信変調部 2 0 5 2 へと出力され、それらを変調部 2 0 0 8、送信ウェイト部 2 0 0 9、送信部 2 0 1 0 を通じて R F 信号が符号化信号として出力される。

【 0 2 1 3 】

基地局は、符号化信号を受信すると受信復調部 1 9 5 0 が受信部 1 9 0 1、復調部 1 9 0 2 を通じて R F 信号を復調信号へと復調する。復号部 1 9 5 1 は復調信号と (2) で求めた符号化パラメータを用い、デインタリーブ、デパンクチャ、デコードの順に復号を行い、データを出力する。

【 0 2 1 4 】

以上のように通信を行うことでデータの授受が行えることが分かる。以上説明したように、符号化パラメータを伝搬状態に対応させて通信を行うことにより、伝搬状態に応じた最適な符号 (復号) が可能となるため、通信品質の向上が見込める。

【 0 2 1 5 】

以上、符号化パラメータを伝搬状態に応じて変化させて通信を行う方法について説明した。ここでは、送信時に伝搬制御を行うものとして説明を行ったが、他の実施の形態でも示されているとおり、これは必須ではない。また、符号化方式

として畳み込み符号を用いる旨説明したが、これに制限されるものではなくブロック符号などを用いても構わない。

【 0 2 1 6 】

符号パラメータとしては、エンコードパターン、パンクチャパターン、インターリーブパターンなどを例に挙げたが、それらの一部は固定して用いることも考えられる。こうすることで符号部・復号部をより簡易に構成することが可能である。この場合、通信品質の向上に最も効果的なものを選択することが重要であるが、例えばパンクチャパターンはデータ容量とエラーレートを大きく左右する重要なパラメータの1つであり、このパターンの変更は最も効果的である事が多い。図22の手順では、(1)と(2)、あるいは(3)と(4)の手順は前後しても構わないことは明白である。

【 0 2 1 7 】

また、基準信号の授受の後に符号化信号の授受を行っているが、例えば基準信号と符号化信号とを同一のフォーマット上に配し、符号化パラメータの選択した後に復号(あるいは符号)を行うような手順としても構わない。この様にデータと符号化パラメータ推定用の基準信号をセットとすることで、より細かな符号化パラメータの選択が可能となるといった特長がある。

【 0 2 1 8 】

従来の方法では、符号化パラメータを通信上でのやりとり(ハンドシェイク)によって授受していたが、このような方法を用いることによって不要になり、効率的な上に伝搬環境に素早く対応できるといった大きな特長を持つ。

【 0 2 1 9 】

さらに、以上の説明において伝搬パラメータに応じて最適な符号化パラメータを変化させる方法について示したが、符号化パラメータのみではなく、変調方式自体(QPSK、16QAM)や、CDMAなどの拡散符号長も変化させることが可能であることは明白である。この様にすることで、符号化パラメータ同様柔軟性に富み、さらに効率野よい通信が提供できるといった有利な特長を備える。

【 0 2 2 0 】

(実施の形態12)

ここでは、伝搬状態推定の精度を向上させる方法と伝搬状態を用いて復調精度を向上させる方法について、図 2 1 および図 2 3 を用いて説明する。

【 0 2 2 1 】

他の実施の形態では、主に伝搬状態を用いたデータ通信について説明を行った。これらは、伝搬状態の推定精度が要求されるといった問題を有している。一般に、推定精度は演算に用いるデータ量に比例するが、データ量が多くなると効率が低下する。また、伝搬推定結果は伝搬推定に用いる基準信号の自己相関にも影響を受ける。これらを解決する手段を図 2 3 を用いて説明する。

【 0 2 2 2 】

図 2 3 は、図 6 に示した伝搬推定部 6 5 0 を詳細に示したものである。2 3 0 1 は受信信号を入力しこれを一時保持するバッファであり、2 3 0 2 は伝搬推定用の基準信号系列を格納した基準信号系列格納部であり、2 3 0 3 は基準信号系列とバッファされた受信信号との畳み込み演算（相関）を行い、1 次遅延プロファイルを算出するコンボルバであり、2 3 0 4 は基準信号系列を入力しその系列の自己相関関数を出力する自己相関演算部であり、2 3 0 5 は 1 次遅延プロファイルをと自己相関関数を入力し、1 次遅延プロファイルから自己相関関数成分を除去した 2 次遅延プロファイルを出力する成分除去部であり、2 3 0 6 は 2 次遅延プロファイルを入力し一定期間の推定結果の平均かを施す平均化演算部である。

以上のように構成された伝搬推定部の動作を説明する。

【 0 2 2 3 】

入力された受信信号を一時保持し、これと基準信号系列とがコンボルバ 2 3 0 3 によって相関値が演算され 1 次遅延プロファイルが出力される。基準信号系列は、自己相関演算部 2 3 0 4 によって自己相関関数が演算されこれが出力される。

【 0 2 2 4 】

遅延プロファイルの演算は

【 0 2 2 5 】

【数16】

$$D_s(t) = \sum (S_r(t+n) \cdot R(n))$$

【0226】

ここで、 D_s が推定した遅延プロファイル、 S_r は受信信号、 R は基準信号系列である。この時、受信信号は送信信号 S_t と伝搬歪 P_d を用いて

【0227】

【数17】

$$S_r(t) = S_t(t) \cdot P_d(t)$$

【0228】

で表すことができ、さらに送信信号 S_t は基準信号であることから

【0229】

【数18】

$$\begin{aligned} D_s(t) &= \sum (S_t(t+n) \cdot P_d(t+n) \cdot R(n)) \\ &= \sum (R(t+n) \cdot P_d(t+n) \cdot R(n)) \end{aligned}$$

【0230】

となる。ここで

【0231】

【数19】

$$A \cdot R(t) = \sum (R(t+n) \cdot R(n))$$

【0232】

を用いると(数18)は

【0233】

【数20】

$$D_s(t) = A \cdot R(t) \cdot \sum P_d(t+n)$$

【 0 2 3 4 】

でとなることがわかる。(数 2 0) で示された通り、ここで求めた遅延プロファイルには、基準信号系列の自己相関関数が含まれているため、これに左右されてしまうことがわかる。成分除去演算部 2 3 0 5 は自己相関演算部 2 3 0 4 が算出した自己相関関数 ($AR(t)$) の成分を一次遅延プロファイルから除去する演算を行う。具体的には、自己相関関数で与えられるインパルス列を IIR フィルタのタップ係数とすることで除去できることが知られている。

【 0 2 3 5 】

さらに、平均化演算部 2 3 0 6 において、複数回演算した結果 (2 次遅延プロファイル) の平均化を施すことによって、歪やノイズにより発生する誤差を抑えることが可能となる。このようにして得られた伝搬推定結果を用いることでより高精度な伝搬状態の推定が可能となるといった有利な特長を有する。

さて、このようにして求めた伝搬推定を用いて有効に復調する方法について図 2 1 を用いて説明する。

【 0 2 3 6 】

図 2 1 は、図 1 の受信復調部 1 5 0 の復調部 1 0 4 に替えて等化復調部 2 1 5 1 にしたものである。2 1 5 1 は、受信信号を入力し信号等化した等化信号を出力する等化部 2 1 0 4 と、等化信号を入力しそれを復調した結果の復調情報を出力する復調部 2 1 0 5 で構成される。

【 0 2 3 7 】

基本的動作は図 1 と変わらないため、相違点のみ説明する。入力された RF 信号が受信部 2 1 0 1 により出力された受信信号は、伝搬推定部 2 1 0 2 によって伝搬状態が推定される。この情報は、受信部 2 1 0 1、等化復調部 2 1 5 1、伝搬情報符号化部 2 1 0 3 へ入力される。伝搬情報符号化部 2 1 0 3 では入力された伝搬情報から特長を抽出し、伝搬特長符号を出力、この結果が等化復調部 2 1 5 1 へと入力される。等化部 2 1 0 4 は推定された伝搬情報と、その特長を示す伝搬特徴符号とを入力し、受信信号から不要成分の除去を行った等化信号を出力する。復調部 2 1 0 5 は、同様に伝搬情報と伝搬特徴符号とから適した復調手段を用いて等化信号を復調、復調情報を出力する。

【0238】

この様に、伝搬情報、伝搬特徴符号を等化復調部2151に入力し、等化あるいは復調に用いることで、それらを有効に利用して効果的な等化・復調が可能になり、結果として通信品質の向上が見込めるといった特長を有する。

【0239】

とくに、受信信号から不要成分（たとえばマルチパス成分など）を除去する等化部2104に、伝搬特徴符号に対応するタップ係数のテーブルを用意しておき、前記符号に対応したタップ係数を用いて等化处理を行うことで、演算量の大幅な削減効果が得られるといった大きな特長がある。その後、伝搬特徴符号と伝搬情報の差分について等化处理を行うことでより簡易な等化处理部の構成が簡単になるといった特長を有する。

【0240】

ここで説明した図23に示す伝搬推定部と、図21に示す受信復調部はそれぞれ独立して受信装置に組み込むことが可能であり、他の実施の形態で示した装置に適用可能であることは明白である。特に、これらを一緒に実施することでより大きな効果が期待できるといった特長を有する。

【0241】

【発明の効果】

以上のように本発明によれば、送信局が推定した伝搬路環境を用いて通信に応用することで、第3者では観測不可能な通信方式を可能にする。また本発明は、従来の通信方式に非常に親和性が高く、変調方式、多重化方式を選ばないため、従来のシステムに最小限の変更を加えるのみでセキュリティ上安全な通信を提供する。また、従来技術である暗号化方式とを組み合わせることで、非常に高いセキュリティを確保することが可能である。

【0242】

この様に、簡易な構成で無線通信の課題となっていたセキュリティを解決するため、その効果は非常に大きい。

【図面の簡単な説明】

【図1】

本発明の一実施の形態における通信装置を示す図

【図 2】

本発明の一実施の形態における通信装置を示す図

【図 3】

本発明の一実施の形態における通信の手続きを示す図

【図 4】

本発明の一実施の形態における通信装置を示す図

【図 5】

本発明の一実施の形態における通信の手続きを示す図

【図 6】

本発明の一実施の形態における伝搬推定部および符号化部を示す図

【図 7】

本発明の一実施の形態における伝搬制御部および変調部、送信部を示す図

【図 8】

本発明の一実施の形態における通信の手続きを示す図

【図 9】

本発明の一実施の形態における通信のフレーム構成を示す図

【図 1 0】

本発明の一実施の形態における通信遷移と制御方式を示す図

【図 1 1】

本発明の一実施の形態における受信装置を示す図

【図 1 2】

本発明の一実施の形態における送信装置を示す図

【図 1 3】

本発明の一実施の形態における到来方向推定部を示す図

【図 1 4】

本発明の一実施の形態における通信装置を示す図

【図 1 5】

本発明の一実施の形態における偏波状態を示す図

【図 1 6】

本発明の一実施の形態における遅延プロファイルを示す図

【図 1 7】

本発明の一実施の形態における到来方向推定結果を示す図

【図 1 8】

本発明の一実施の形態におけるコードブックの内容を示す図

【図 1 9】

本発明の一実施の形態における受信装置の一部を示す図

【図 2 0】

本発明の一実施の形態における送信装置の一部を示す図

【図 2 1】

本発明の一実施の形態における受信復調部を示す図

【図 2 2】

本発明の一実施の形態における通信の手続きを示す図

【図 2 3】

本発明の一実施の形態における伝搬推定部を示す図

【符号の説明】

- 1 0 1、2 0 1、4 0 1 アンテナ
- 1 0 2、2 0 2、4 0 2 受信部
- 1 0 3、2 0 3、4 0 3 伝搬推定部
- 1 0 4、2 0 4、4 0 4 復調部
- 1 0 5、2 0 5、4 0 5 符号化部
- 1 0 6、2 0 6、4 0 6 バッファ
- 1 0 7、4 0 7、4 0 7 復号化部
- 1 0 8、2 0 8、4 0 8 基準信号生成部
- 1 0 9、2 5 2、4 5 2 送信変調部
- 2 0 9、4 0 9 暗号化部
- 2 1 0、4 1 0 切換部
- 4 1 1 伝搬制御部

2 1 1、4 1 2 変調部

1 5 0、2 5 0、4 5 0 受信復調部

1 5 1、2 5 1、4 5 1 暗号鍵生成部

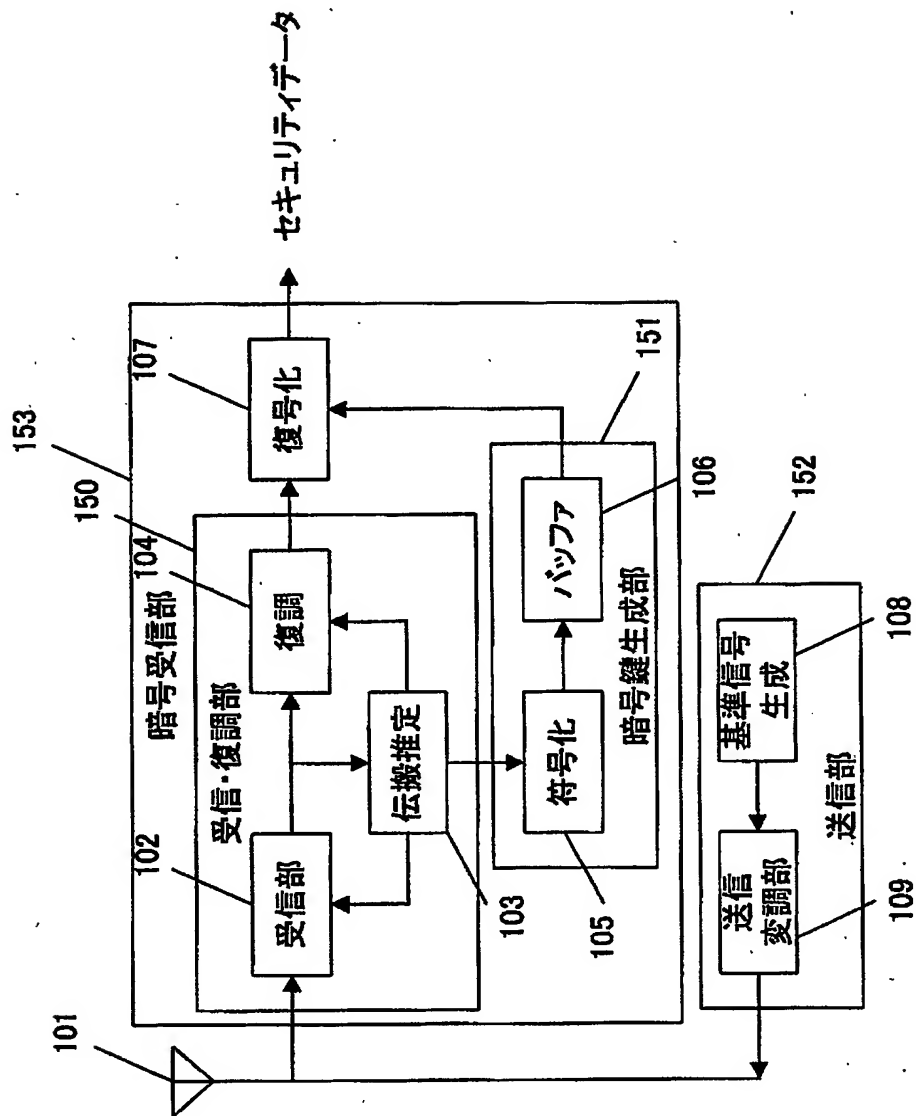
1 5 2、2 1 2、4 1 3 送信部

1 5 3、2 5 3、4 5 3 暗号受信部

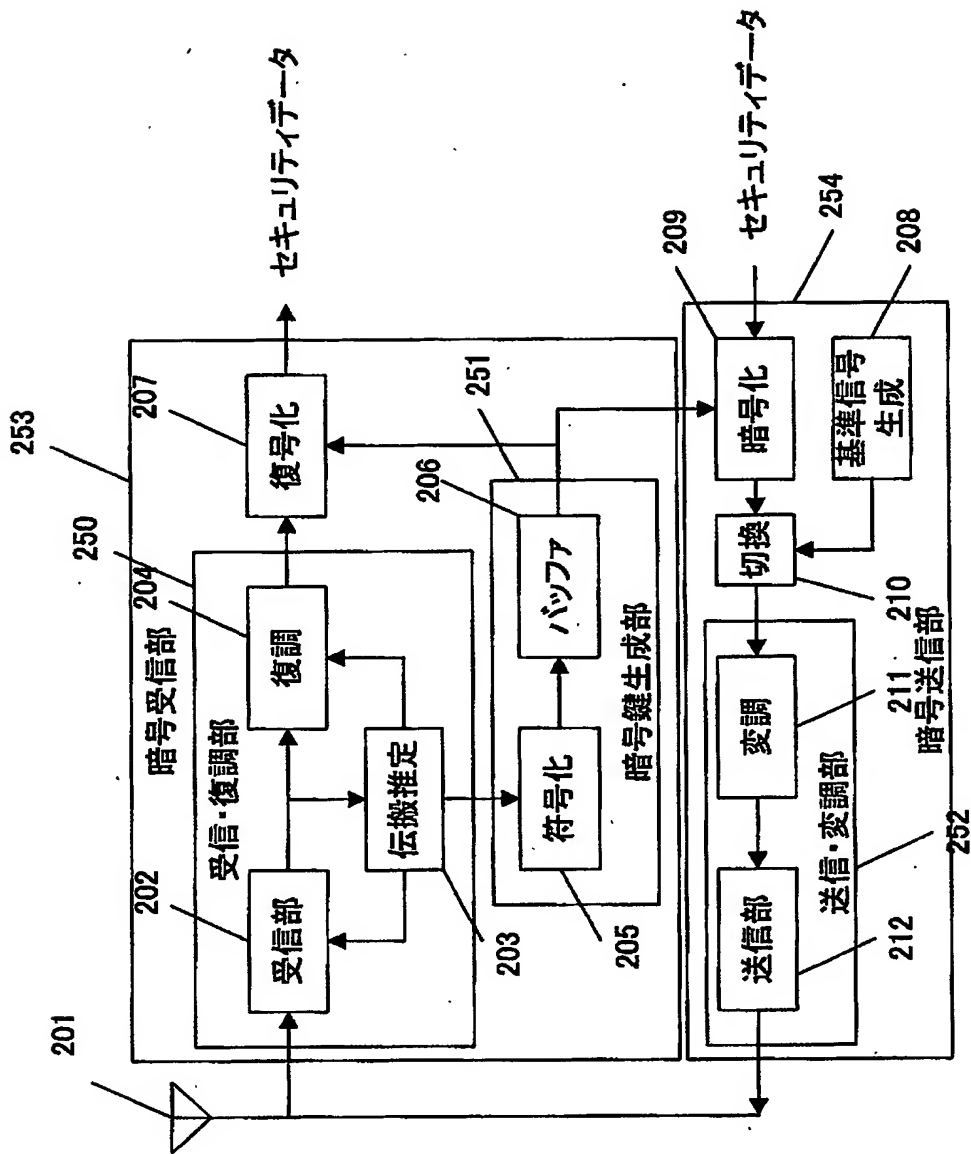
【書類名】

図面

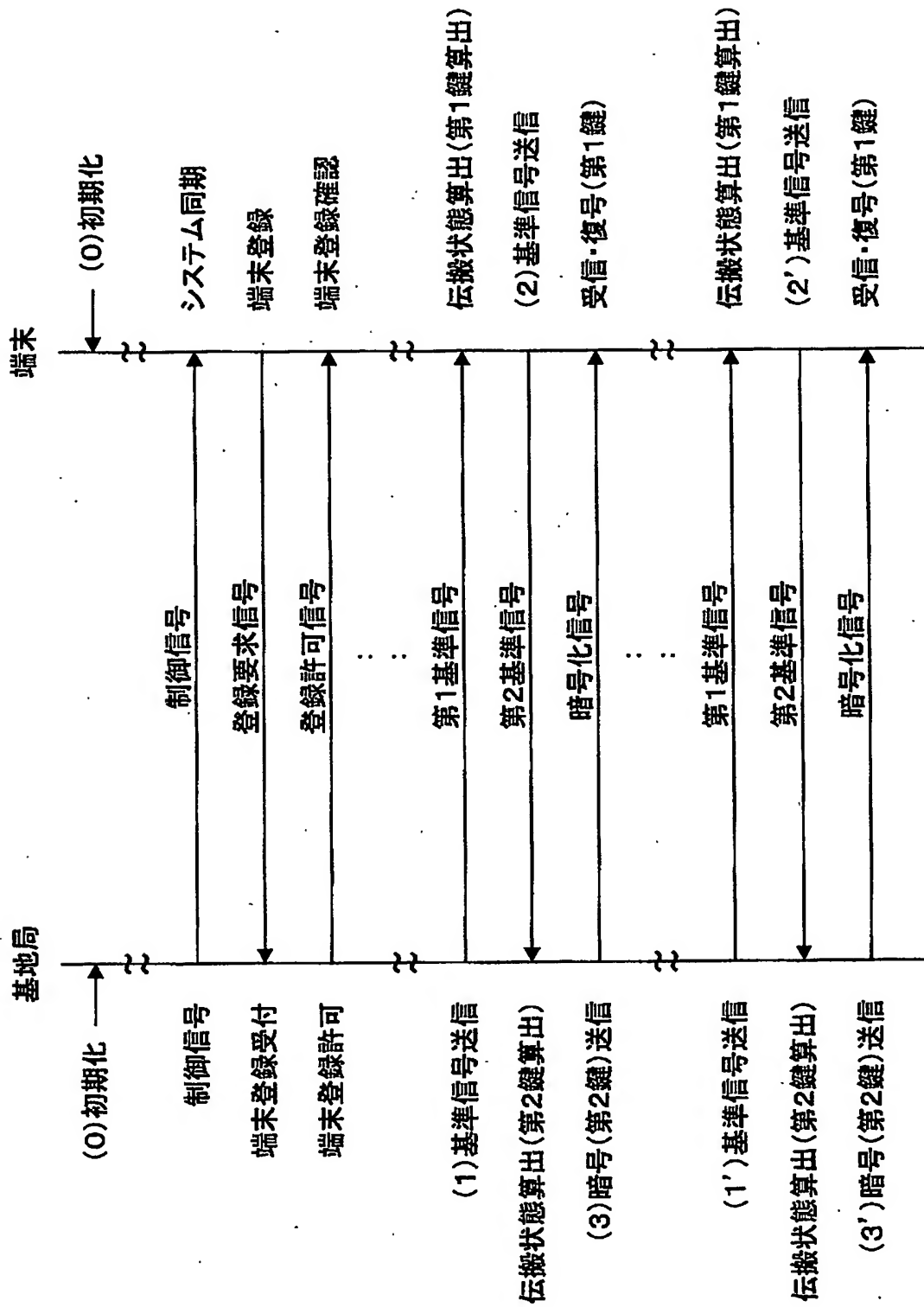
【図 1】



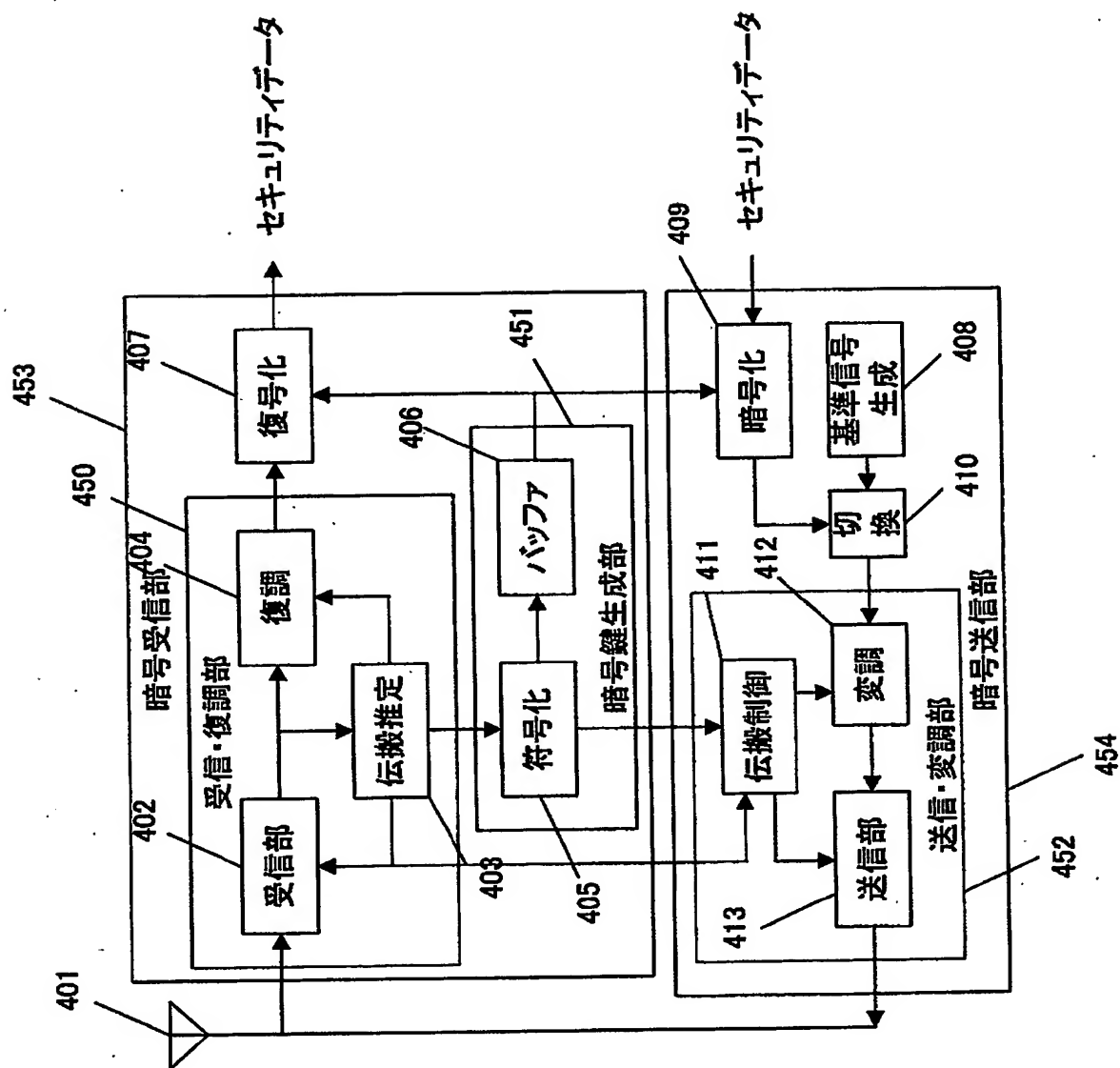
【図2】



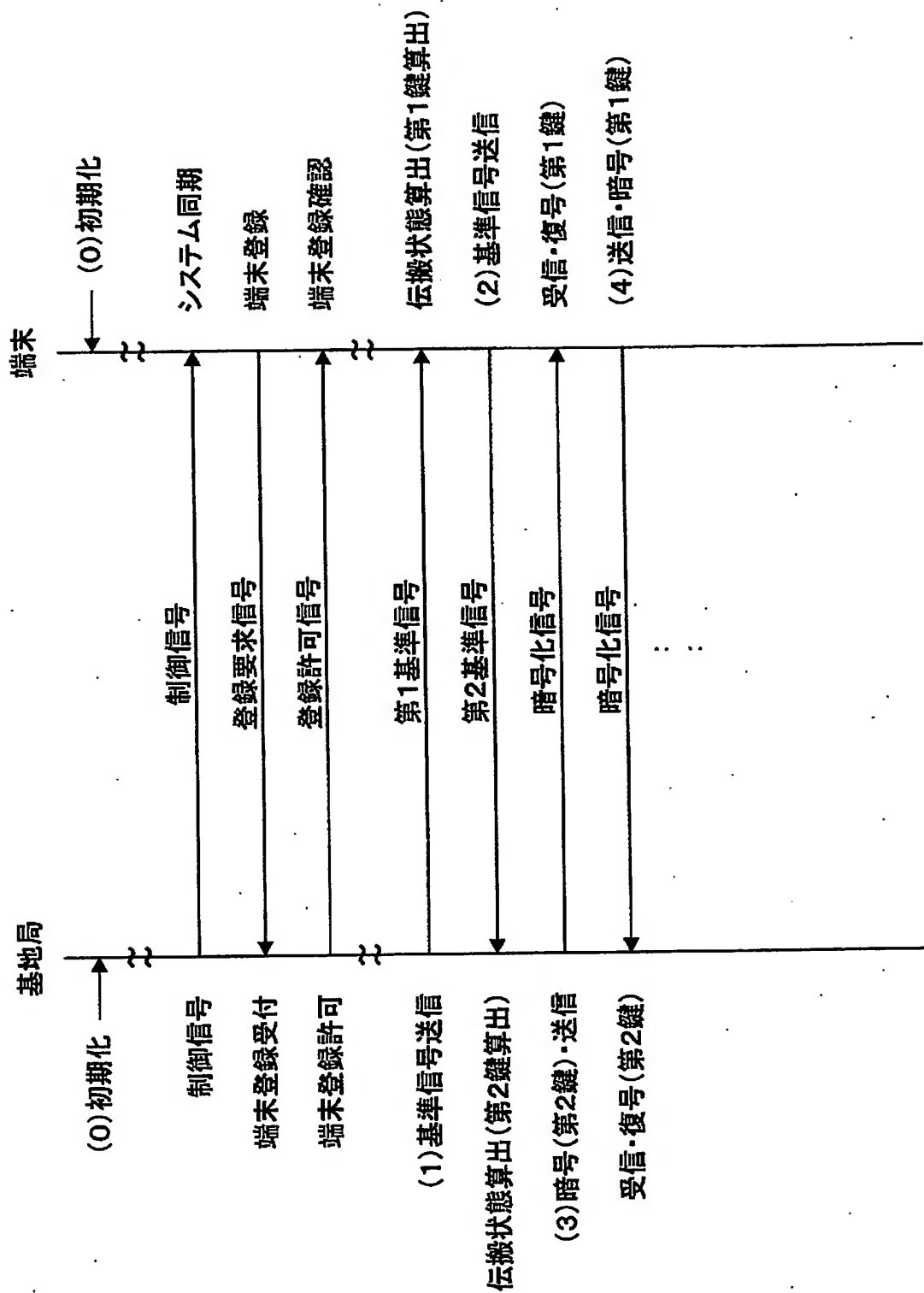
【図 3】



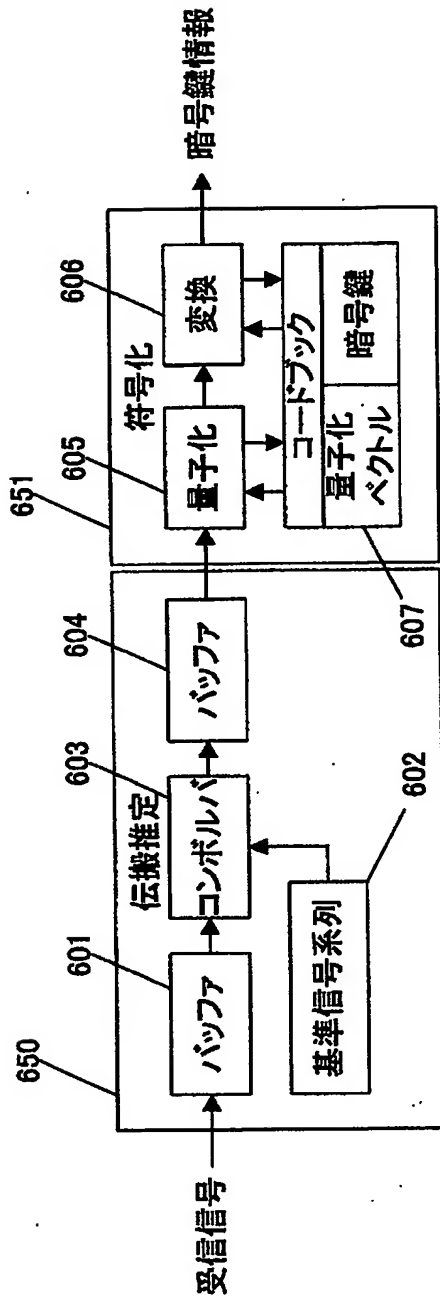
【図 4】



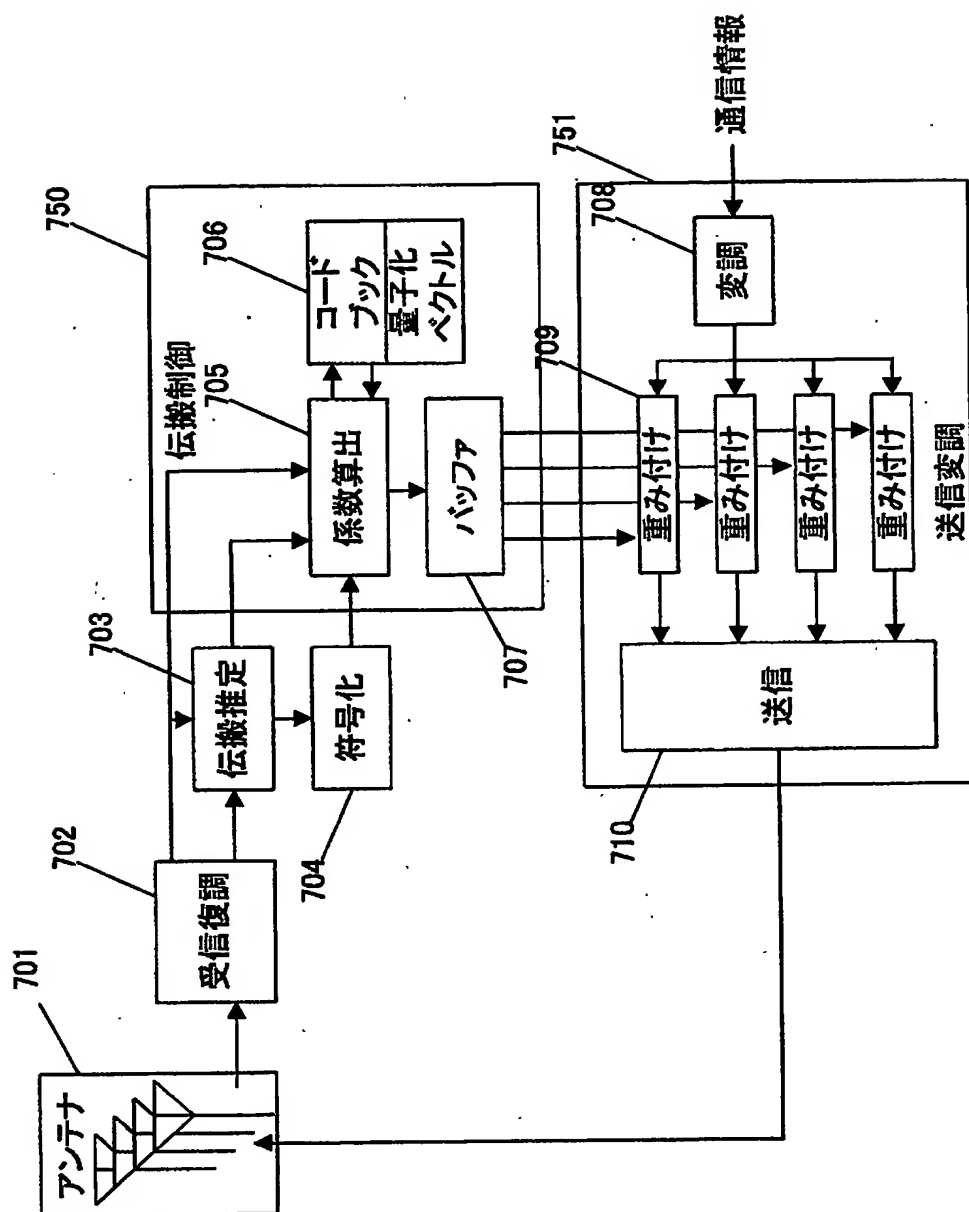
【図 5】



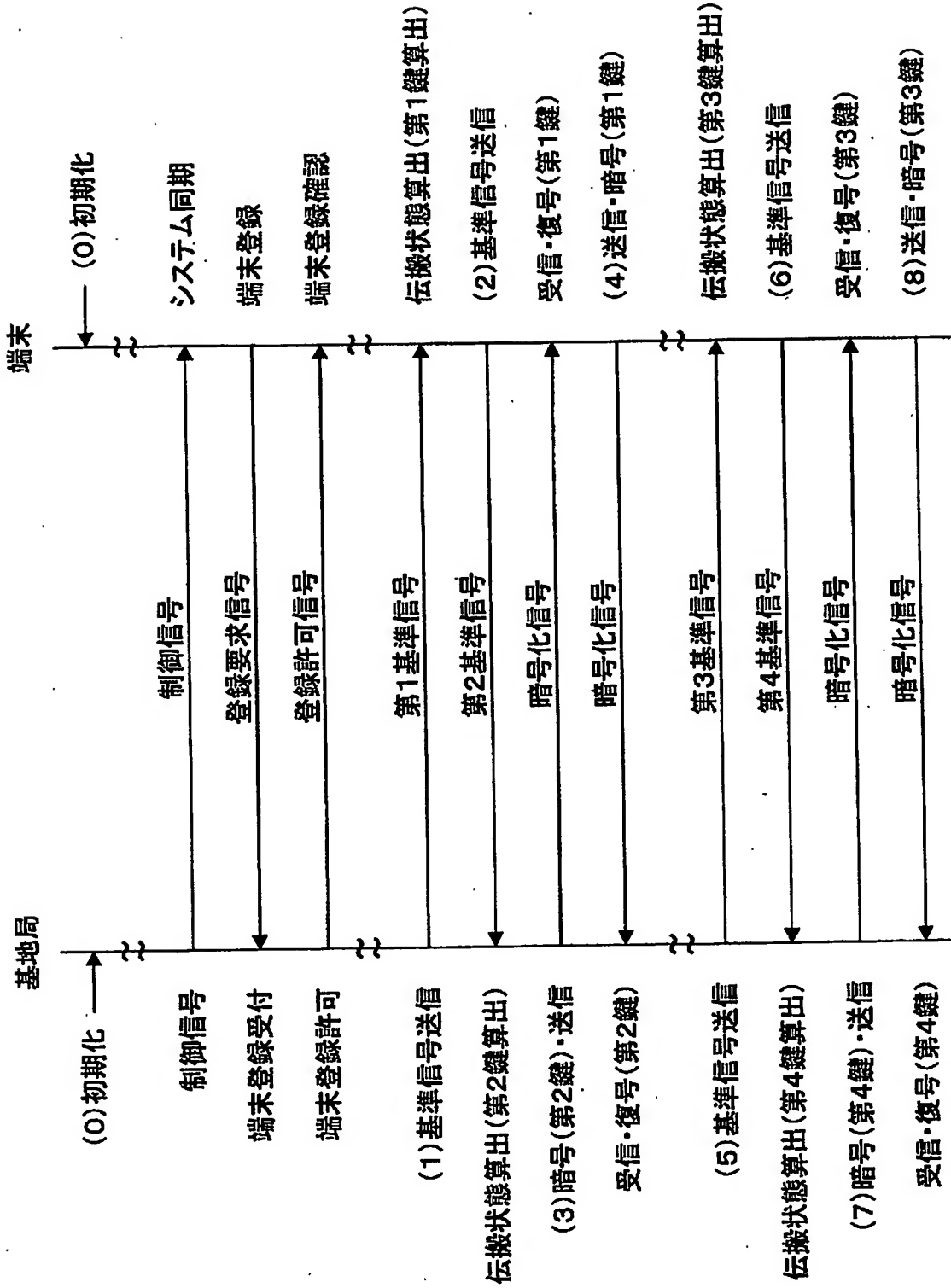
【図 6】



【图 7】



【図 8】

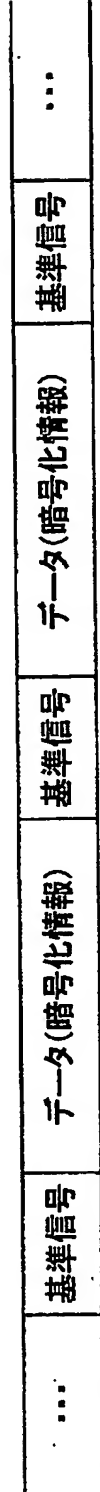


【図9】

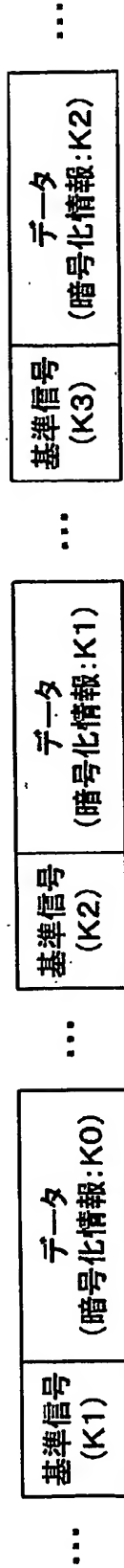
フレーム構成(a)



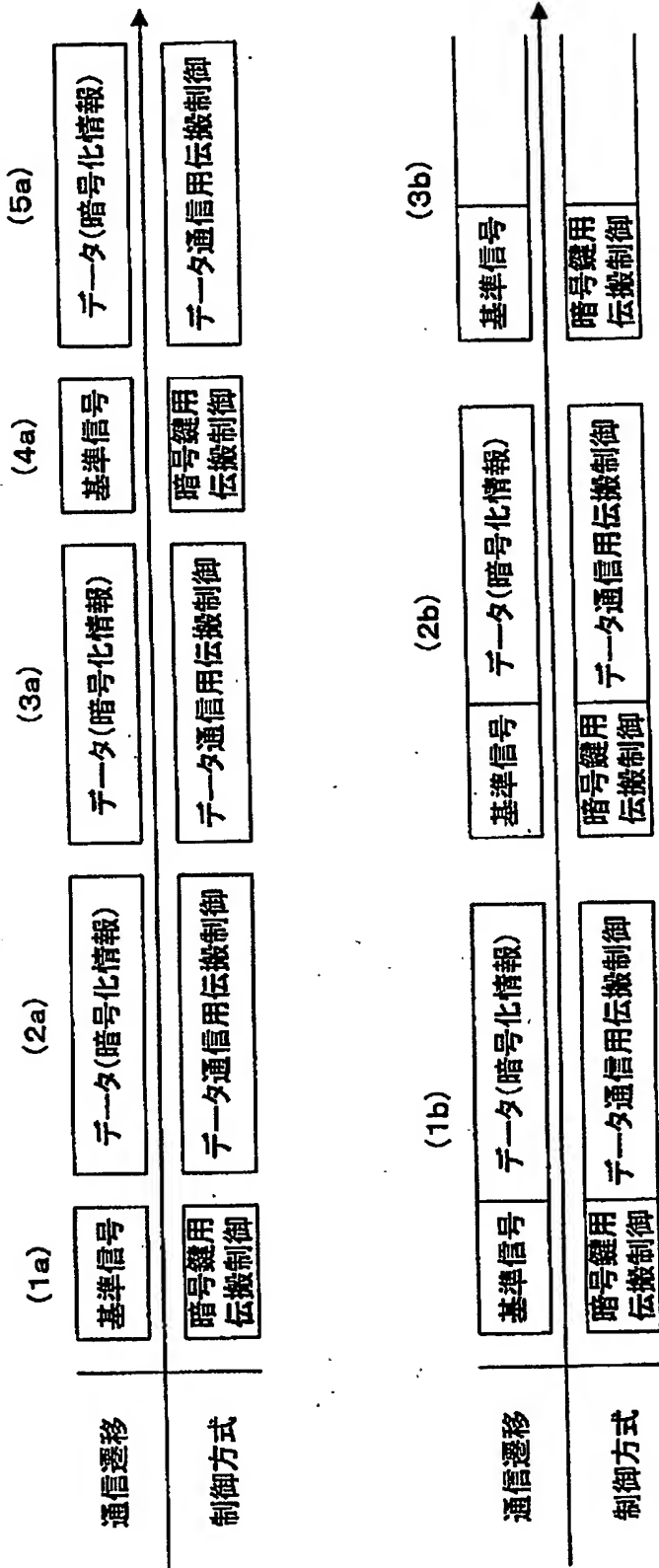
フレーム構成(b)



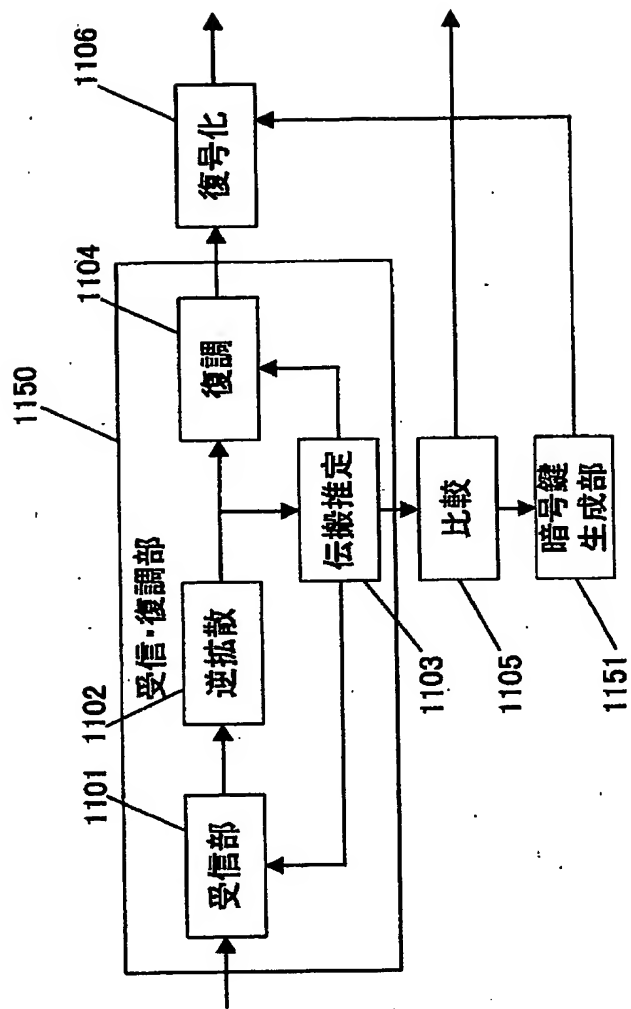
フレーム構成(c)



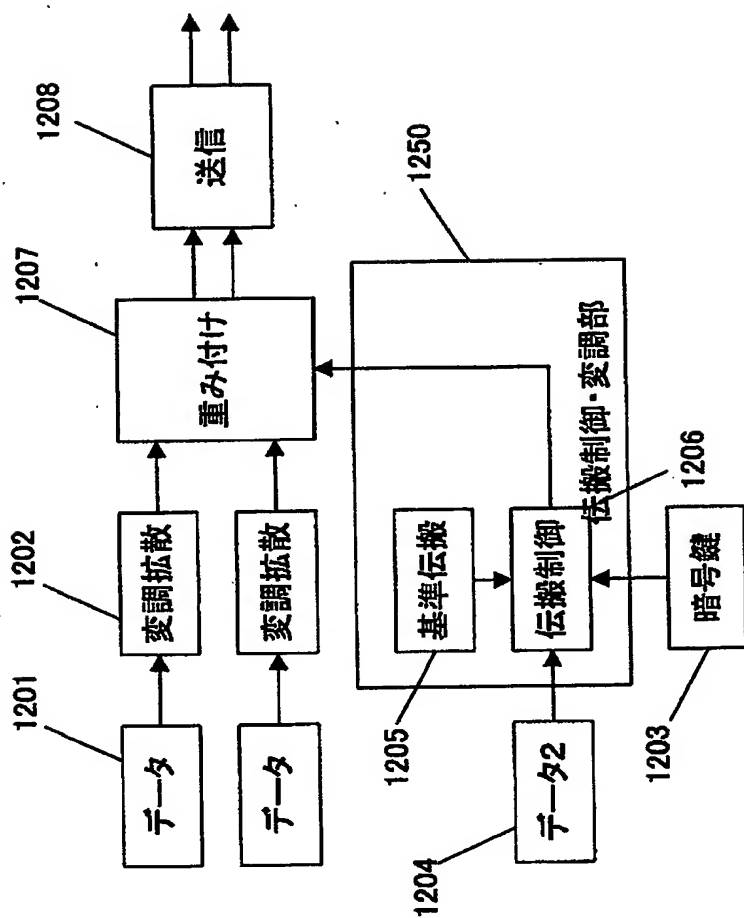
【図 10】



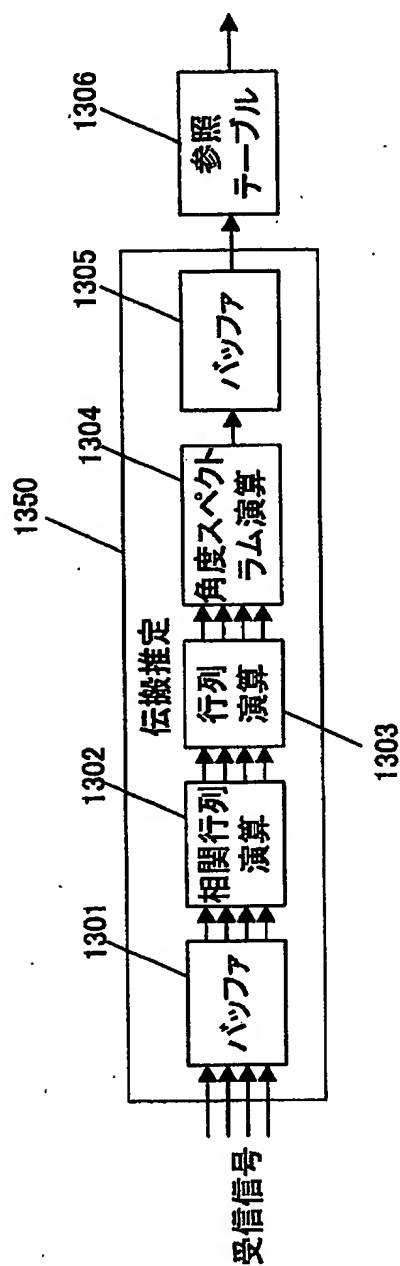
【図 11】



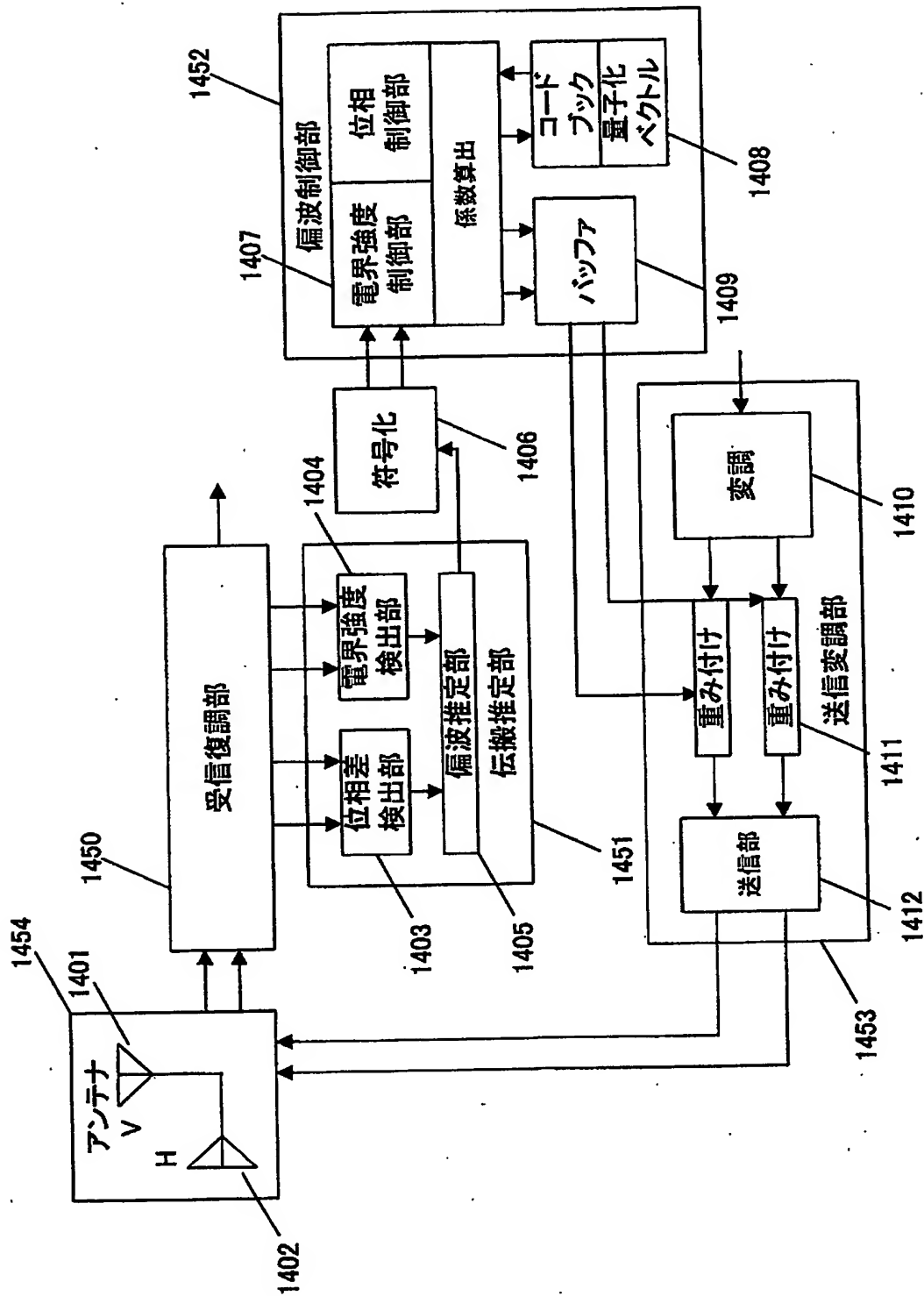
【図 12】



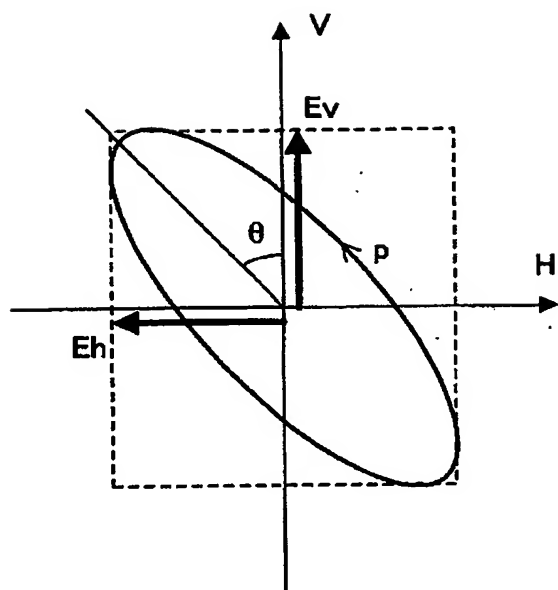
【図 13】



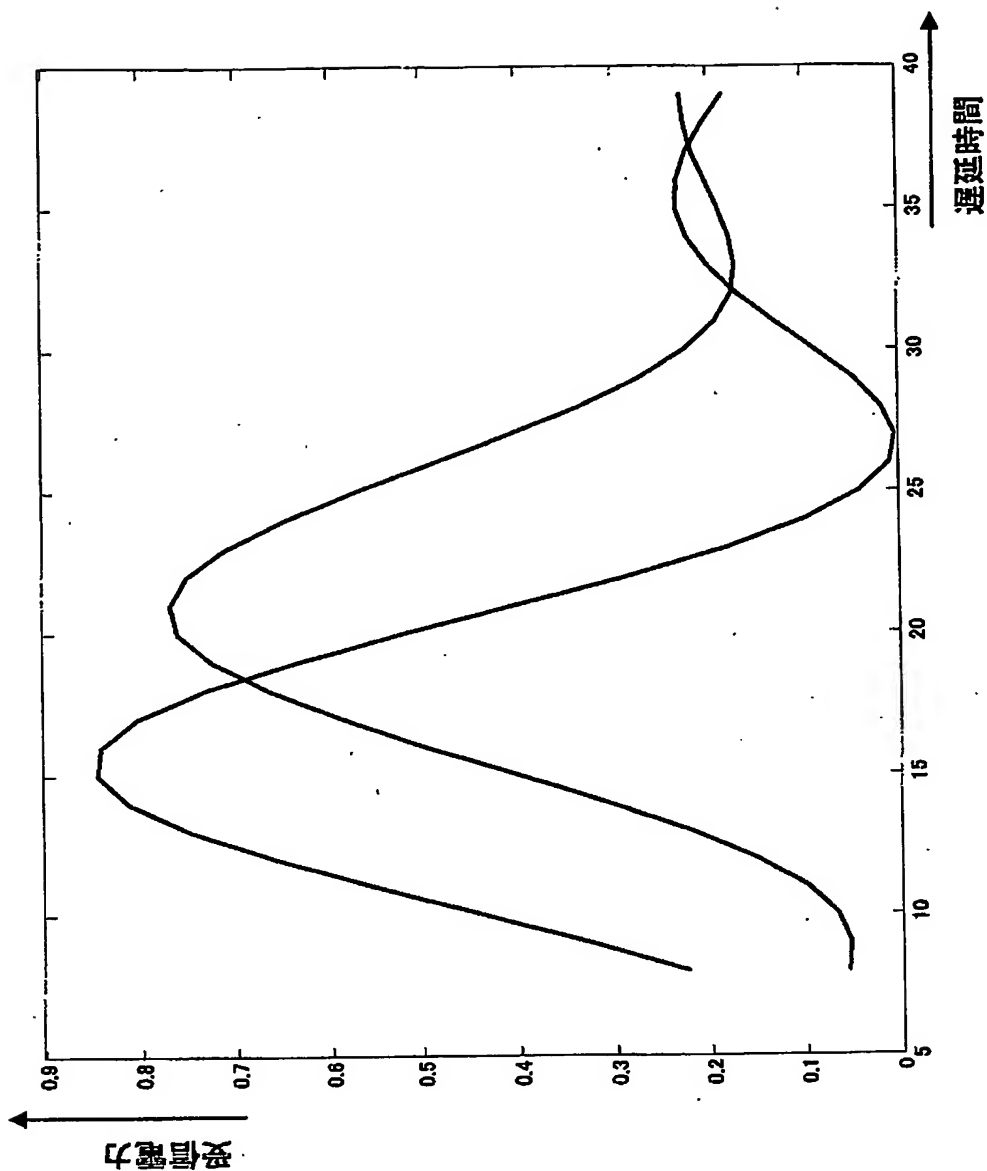
【図 14】



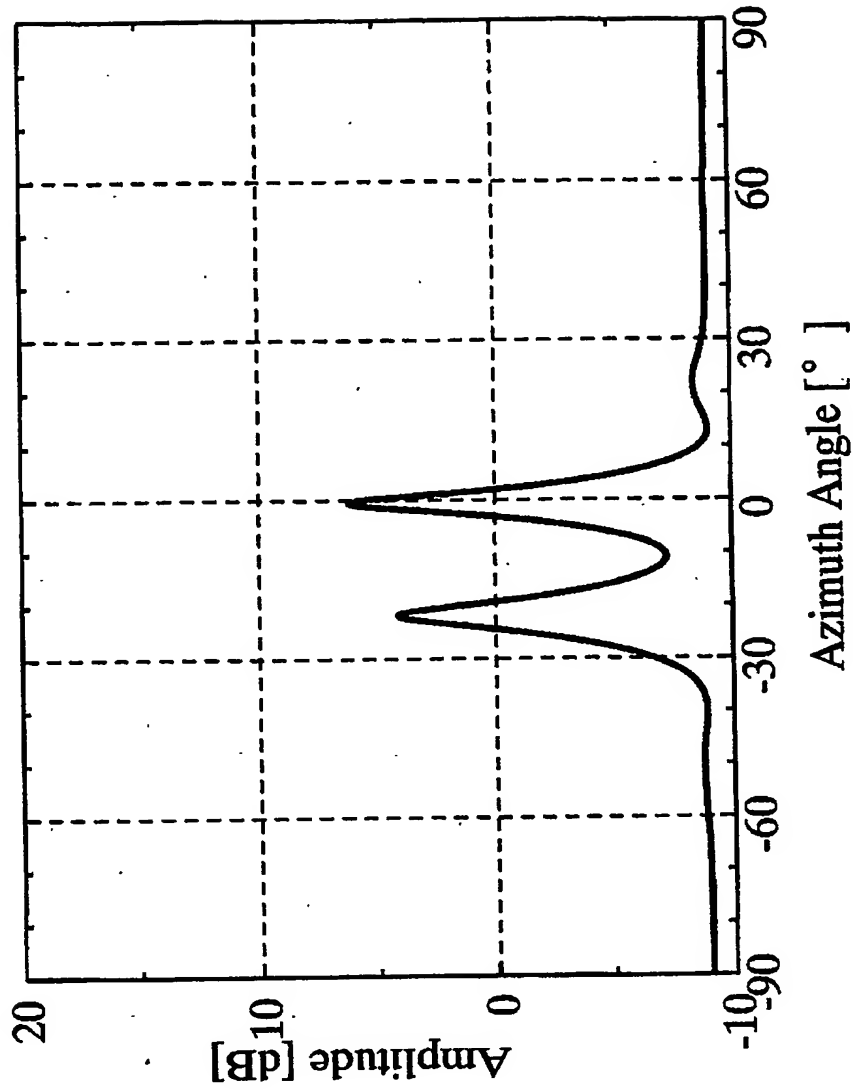
【図 15】



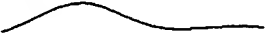







【図16】



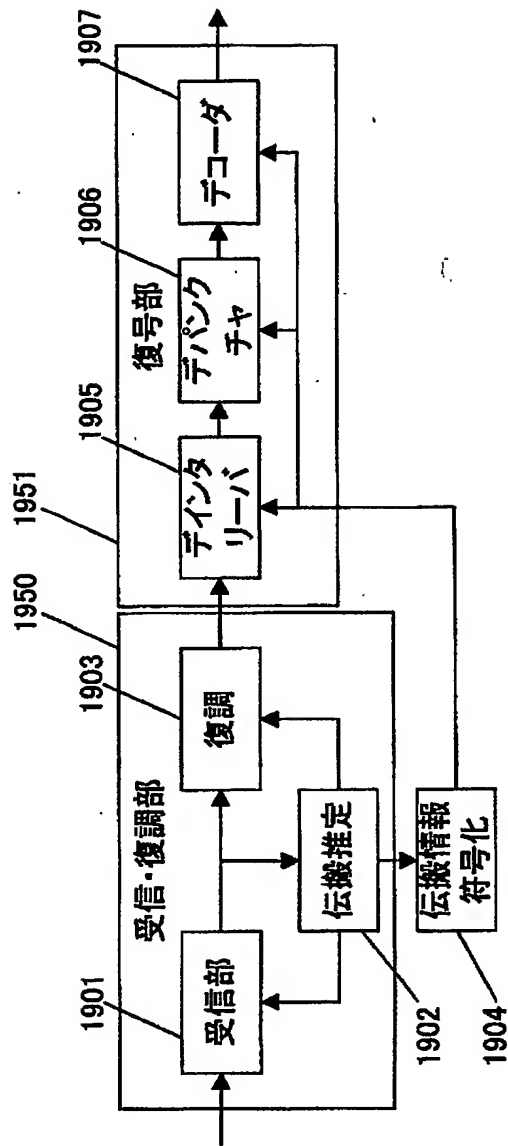
【図 17】



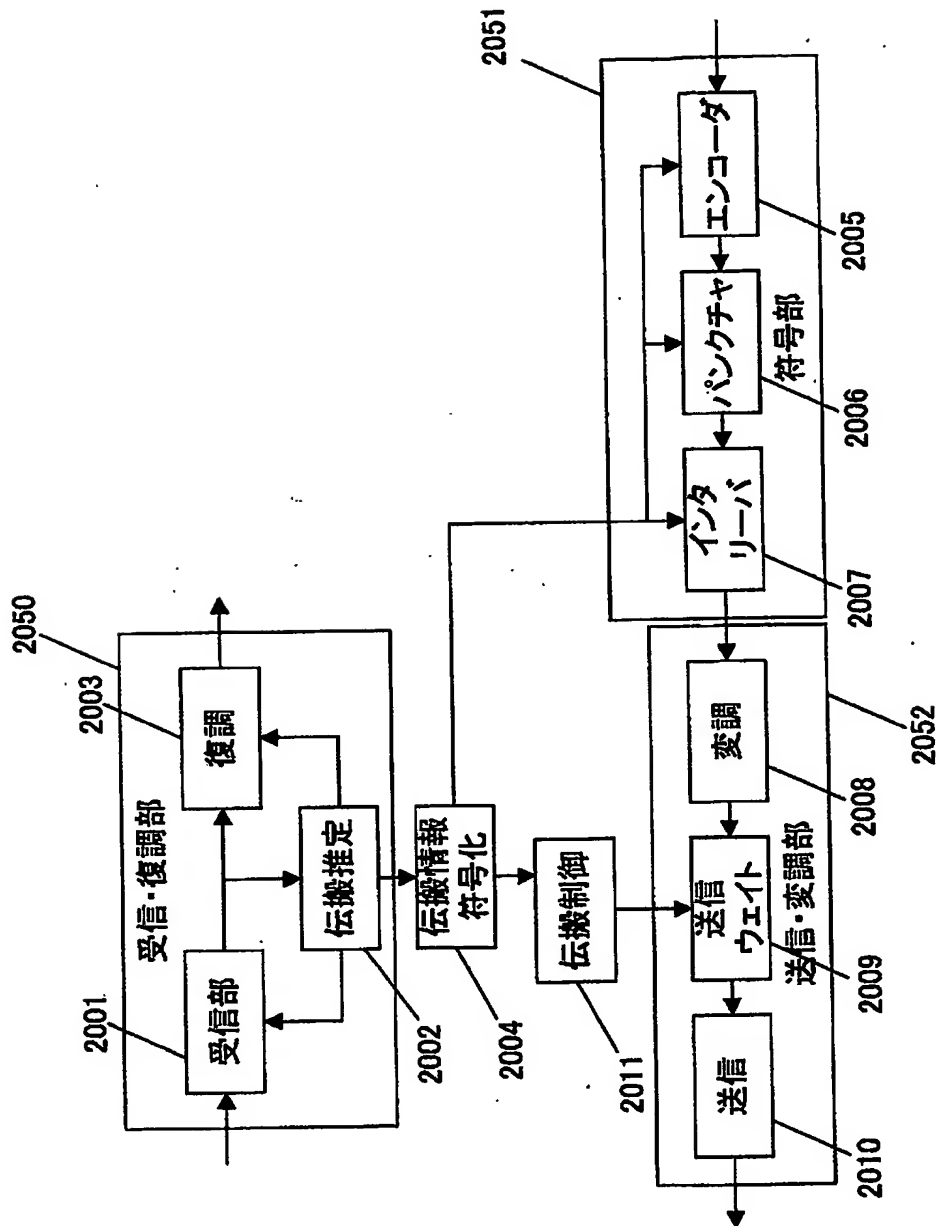
【図 18】

コードブック	
量子化ベクトル	暗号鍵
	aAnPoCgk
	Yncwkopq
	BemkingT
	qCTuNVpz
	RkPoCvvW
	uCqDGwpo
	LfUUfEzc
	llueGenc
⋮	⋮

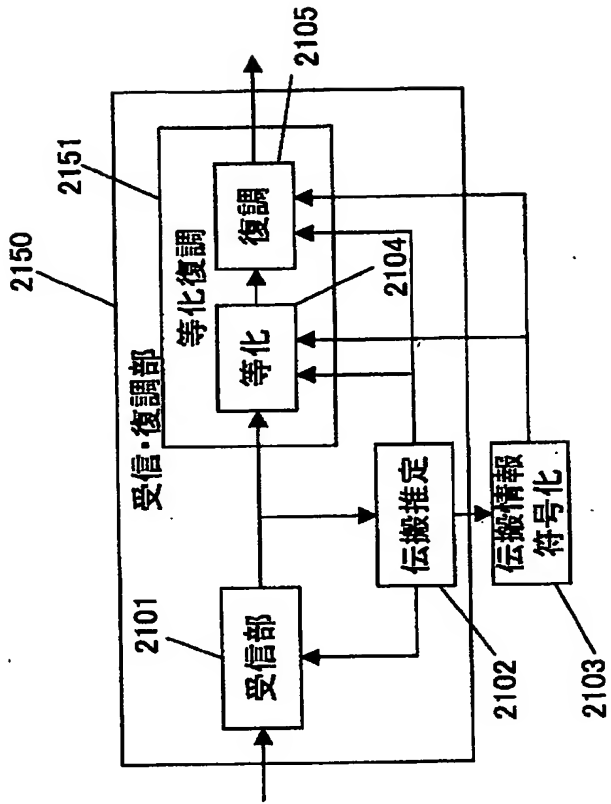
【図 19】



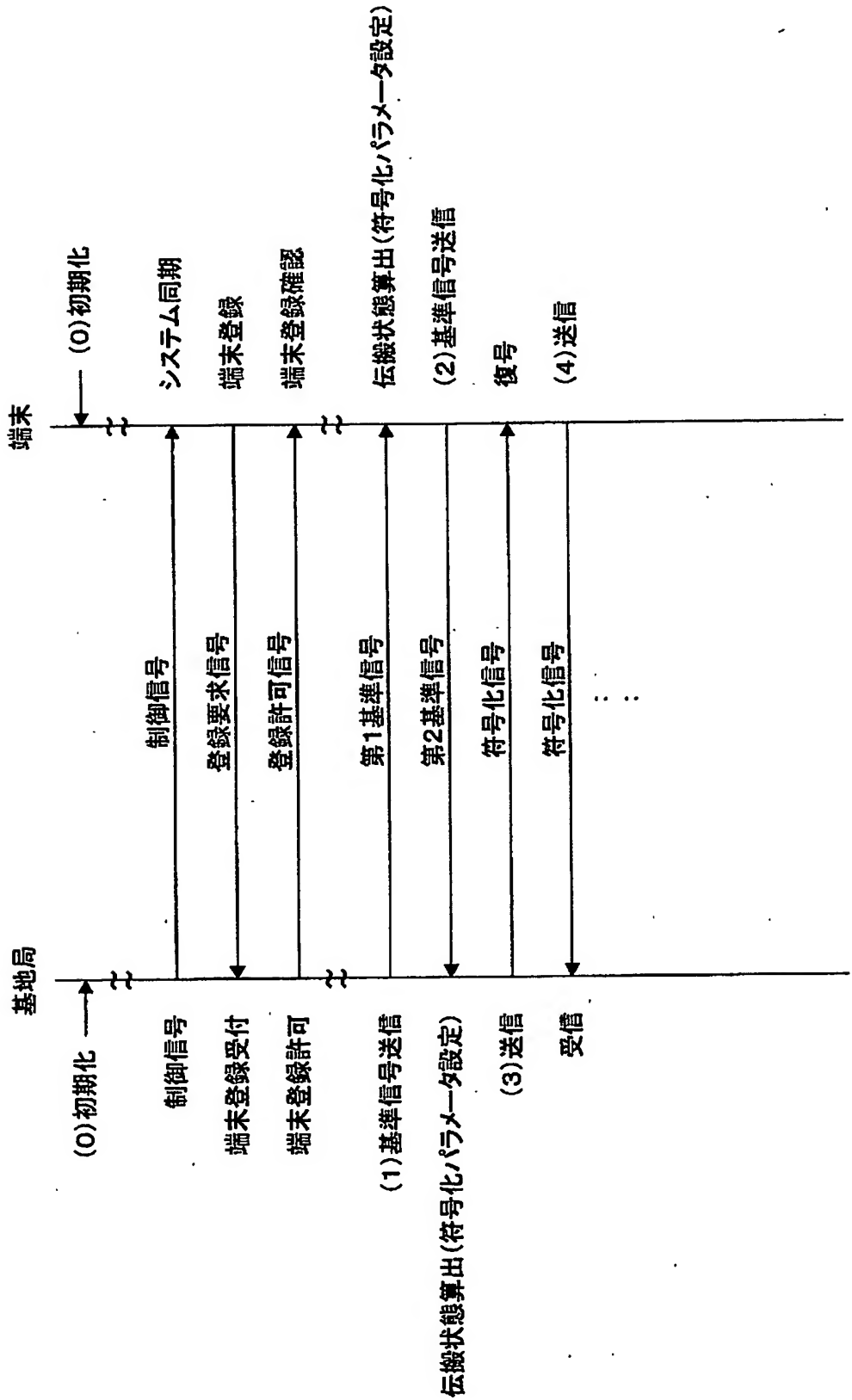
【図 20】



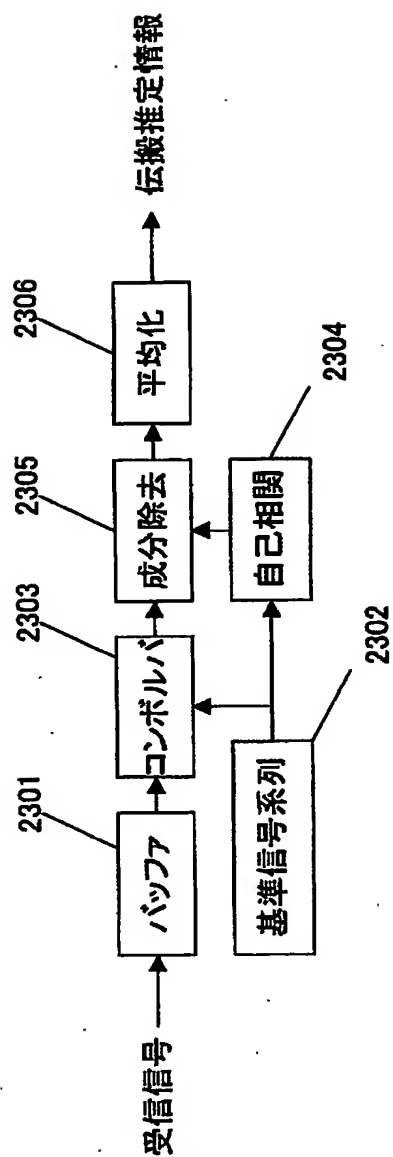
【図 21】



【図 2 2】



【図 23】



【書類名】 要約書

【要約】

【課題】 無線通信の傍受による、情報の漏洩が生じる。

【解決手段】 通信当事者のみが知る伝搬路環境を用いることで、第3者が通信内容を傍受しても復調不可能となる通信方式を提供する。基地局は伝搬路推定用に基準信号を発信する。端末はそれを受信し伝搬路推定を行い、具備されたコードブック中の最も類似した伝搬状態に対応した暗号鍵（第1鍵）を設定する。次に、端末は伝搬路推定用に基準信号を発信する。基地局はそれを受信し伝搬路推定を行い、具備されたコードブック中の最も類似した伝搬状態に対応した暗号鍵（第2鍵）を設定する。以後、基地局は第1鍵で暗号化したデータを送信し、端末は第2鍵で受信したデータを復号する。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社